(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－252183

(43)公開日　平成11年(1999)９月17日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ
Ｈ０４Ｂ　7/24		Ｈ０４Ｂ　7/24	Ａ
Ｈ０４Ｑ　7/38		Ｈ０４Ｍ　3/00	Ｂ
Ｈ０４Ｌ　12/28		11/00	３０３
12/46		Ｈ０４Ｂ　7/26	１０９Ｍ

審査請求　未請求　請求項の数５　ＯＬ　外国語出願　（全168頁）　最終頁に続く

(21)出願番号　特願平10－306438

(22)出願日　平成10年(1998)10月14日

(31)優先権主張番号　６０／０６１９１５

(32)優先日　1997年10月14日

(33)優先権主張国　米国（ＵＳ）

(31)優先権主張番号　０９／１３８９０３

(32)優先日　1998年８月24日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　596092698
ルーセント　テクノロジーズ　インコーポレーテッド
アメリカ合衆国．07974－0636　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　600

(72)発明者　ピレツ　モッシュズ　フェーダー
アメリカ合衆国　07631　ニュージャーシィ，イングルウッド，スターリング　ロード　300

(74)代理人　弁理士　岡部　正夫　(外11名)

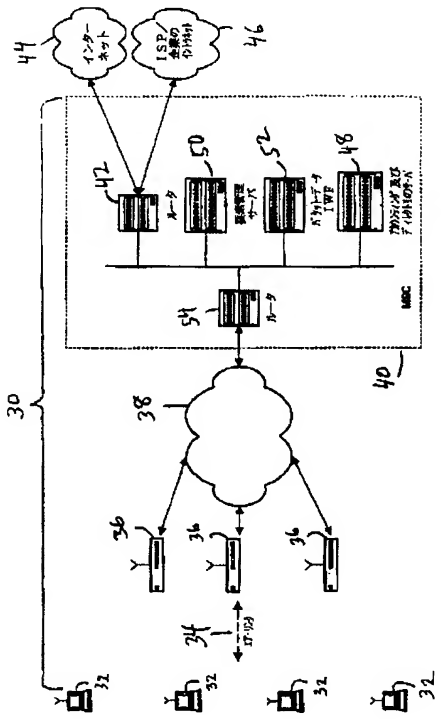
最終頁に続く

(54)【発明の名称】　イーサネット（登録商標）フレームにおけるポイント・ツー・ポイント・プロトコルのカプセル化

(57)【要約】

【課題】　本発明は、無線データ・ネットワークに関し、無線データ・ネットワークにおけるピア・ツー・ピア・プロトコルのサーバによる通信に関する技術を提供する。

【解決手段】　本発明は、無線データ・ネットワークであって、ホーム移動交換センターと、無線モデムおよび少なくとも１つのエンド・システムとを含み、該無線モデムおよび該少なくとも１つのエンド・システムはイーサネット・リンク経由で互いに接続されているホーム・ネットワークと、ＰＰＰサーバとを含み、該ＰＰＰサーバから該少なくとも１つのエンド・システムに対して送信されるＰＰＰ情報は、イーサネット・フレームの中に無線モデムによってカプセル化され、そして該少なくとも１つのエンド・システムに対して該イーサネット・リンク経由で送信されるようになっていることを特徴とする。



1

【特許請求の範囲】

【請求項１】　無線データ・ネットワークであって、ホーム移動交換センターと、無線モデムおよび少なくとも１つのエンド・システムとを含み、該無線モデムおよび該少なくとも１つのエンド・システムはイーサネット・リンク経由で互いに接続されているホーム・ネットワークと、

ＰＰＰサーバとを含み、該ＰＰＰサーバから該少なくとも１つのエンド・システムに対して送信されるＰＰＰ情報は、イーサネット・フレームの中に無線モデムによってカプセル化され、そして該少なくとも１つのエンド・システムに対して該イーサネット・リンク経由で送信されるようになっている無線データ・ネットワーク。

【請求項２】　請求項１に記載のネットワークにおいて、該少なくとも１つのエンド・システムからのＰＰＰ情報が、無線モデムに対してイーサネット・リンク経由で送信され、そして次に該無線モデムから該ＰＰＰサーバに対して送信されるようになっているネットワーク。

【請求項３】　請求項１に記載のネットワークにおいて、該ホーム移動交換センターはホーム・インターワーキング機能を含むネットワーク。

【請求項４】　請求項３に記載のネットワークにおいて、該ＰＰＰサーバからのＰＰＰ情報が、該ホーム・インターワーキング機能を通じて該無線モデムに対して送信されるようになっているネットワーク。

【請求項５】　請求項４に記載のネットワークにおいて、該少なくとも１つのエンド・システムからのＰＰＰ情報が、イーサネット・リンク経由で無線モデムに対して送信され、そして次に該無線モデムからＰＰＰサーバに対して該ホーム・インターワーキング機能を通じて送信されるようになっているネットワーク。

【発明の詳細な説明】

【０００１】

【発明の分野】本発明は、無線データ・ネットワークに関し、特に無線データ・ネットワークにおけるピア・ツー・ピア・プロトコルのサーバによる通信に関する。

【０００２】

【従来技術】図１には３つのビジネス・エンティティが示されており、その協力して動作している機器は、通常、ユーザのコンピュータ２に対してモデム４を通じてのリモートのインターネット・アクセスを提供する。ユーザのコンピュータ２およびモデム４は、エンド・システムを構成する。第１のビジネス・エンティティはダイヤルアップのプレイン・オールド・テレフォン・システム（ＰＯＴＳ）、または統合化サービス・データ・ネットワーク（ＩＳＤＮ）を所有していて稼働させている電話会社（ｔｅｌｃｏ）である。ｔｅｌｃｏはユーザと他の２つのビジネス・エンティティとの間にビット（またはパケット）を流すことができる、公衆交換電話網（ＰＳＴＮ）６の形式での伝送媒体を提供する。

2

【０００３】第２のビジネス・エンティティは、インターネット・サービス・プロバイダ（ＩＳＰ）である。ＩＳＰはそのサービス・エリアの中に１つまたはそれ以上のポイント・オブ・プレゼンス（ＰＯＰ）８を配備していて、それを管理し、それに対してエンド・ユーザがネットワーク・サービスを求めて接続する。ＩＳＰは、通常、そのＩＳＰへの加入者があることを期待して、主要な各呼出しエリアの中にＰＯＰを設立する。ＰＯＰはＰＳＴＮからのメッセージ・トラヒックを、イントラネット・バックボーン１０上で搬送されるディジタル形式に変換する。イントラネット・バックボーン１０はＩＳＰによって所有されているか、ＭＣＩ、Ｉｎｃ．などのイントラネット・バックボーン・プロバイダからリースされるかのいずれかである。ＩＳＰは、通常、ＰＳＴＮに対する接続のためにｔｅｌｃｏからの部分的またはフルのＴ１またはＴ３回線をリースする。ＰＯＰおよびＩＳＰのメディア・データ・センター１４はルータ１２Ａを通じてイントラネットのバックボーン上で一緒に接続されている。データ・センターはＩＳＰのウェブ・サーバ、メール・サーバ、アカウティングおよび登録のサーバを収容し、ＩＳＰがウェブ・コンテンツ、ｅメールおよびウェブ・ホスティング・サービスをエンド・ユーザに対して提供できるようにする。将来の付加価値サービスはデータ・センターの中に追加のタイプのサーバを配備することによって追加することができる。また、ＩＳＰはパブリック・インターネット・バックボーン２０に接続するためにルータ１２Ａを維持している。リモート・アクセスのための現在のモデルにおいては、エンド・ユーザはそれぞれのｔｅｌｃｏおよびそれぞれのＩＳＰの両方とのサービス関係を有するのが普通であり、通常は、それぞれから別々に料金が請求される。エンド・ユーザは最寄りのＰＯＰをダイヤルすることによって、そしてインターネット・エンジニアリング・タスク・フォース（ＩＥＴＦ）のポイント・ツー・ポイント・プロトコル（ＰＰＰ）として知られている通信プロトコルを実行することによって、ＩＳＰにアクセスし、そのＩＳＰを通してパブリック・インターネット２０にアクセスする。

【０００４】第３のビジネス・エンティティは、ビジネスの理由のためにルータ１２Ｂを通しての自分自身のプライベート・イントラネット１８を所有していて、それを稼働させている私企業である。企業の従業員は企業のリモート・アクセス・サーバ１６に対してＰＯＴＳ／ＩＳＤＮの呼出しを行い、そしてＩＥＴＦのＰＰＰプロトコルを実行することによって企業のネットワーク１８にリモートに（たとえば、自分の家から、あるいは路上にいる間に）アクセスすることができる。企業にアクセスする場合、エンド・ユーザは企業のリモート・アクセス・サーバ１６に接続するコストだけを支払う。ＩＳＰは関与されない。その私企業はエンド・ユーザを企業のイ

ントラネット１８またはパブリック・インターネット２０のいずれかまたはその両方に対して接続するためにルータ１２Ｂを維持している。

【０００５】エンド・ユーザは現在は電話をかけるための費用と、自分の家への電話回線の費用の両方をｔｅｌｃｏに支払う。また、エンド・ユーザはＩＳＰのネットワークおよびサービスにアクセスするための費用もＩＳＰに対して支払う。本発明は、Ｓｐｒｉｎｔ　ＰＣＳ、ＰｒｉｍｅＣｏなどの無線サービス・プロバイダに利点を提供し、ＡＯＬ、ＡＴ＆ＴのＷｏｒｌｄｎｅｔなどのインターネット・サービス・プロバイダにも利点を提供する。

【０００６】現在、インターネット・サービス・プロバイダはインターネット・アクセス・サービス、ウェブ・コンテンツ・サービス、ｅメール・サービス、コンテンツ・ホスティング・サービス、およびローミング（ｒｏａｍｉｎｇ）をエンド・ユーザに対して提供する。マージンが低く、機能および価格に基づいたマーケット・セグメンテーションを行う余地がないので、ＩＳＰはマージンを改善するための付加価値サービスを探している。短期的には、機器のベンダーはＩＳＰがより高速のアクセス、バーチャル・プライベート・ネットワーキング（パブリック・ネットワークをプライベート・ネットワークとして安全に使うための機能およびイントラネットに接続する機能）、ローミング・コンソーシアム、プッシュ・テクノロジおよび特定のサービスの品質を提供できるようにするためのソリューションを、ＩＳＰに対して提供できるようになる。長期的には、インターネットおよびモビリティ上で音声を提供することになる。そのとき、ＩＳＰはこれらの付加価値サービスを使って低マージンの束縛から脱出できるようになる。これらの付加価値の多くはネットワーク・サービスのカテゴリーに入り、そしてネットワークのインフラストラクチャ機器を通じてのみ提供することができる。他の付加価値サービスはネットワークのインフラストラクチャからのサポートを必要とするアプリケーション・サービスのカテゴリーに落ち、一方、他のものはネットワーク・インフラストラクチャからのサポートを必要としない。より速いアクセス、バーチャル・プライベート・ネットワーク、ローミング、モビリティ、音声、サービスの品質、およびＱＯＳベースのアカウンティングなどのサービスはすべて、高度化されたネットワーク・インフラストラクチャを必要とする。ここで記述されているシステムは、これらの高度化されたサービスを直接提供するか、あるいはこれらのサービスを将来の機能強化として後で追加するための手がかりを提供するかのいずれかとなる。無線サービスのプロバイダは歳入のより大きなシェアを獲得することができる。そのＩＳＰはより多くのサービスを、より良いマーケット・セグメンテーションによって提供することができる。

【０００７】

【発明の概要】本発明は、パブリック・インターネット、プライベート・イントラネットおよびインターネット・サービス・プロバイダに対するリモート無線アクセスをエンド・ユーザに提供する。無線のアクセスはホーム・ネットワークの中の基地局および交換の契約を結んでいるフォーリン・ネットワークの中の基地局を通じて提供される。

【０００８】本システムの１つの目的は、モビリティの管理をローカル、マイクロ、マクロ、およびグローバルのコネクションのハンドオーバ・カテゴリーに分割し、そのハンドオーバ・カテゴリーに従ってハンドオフの更新を最小化する無線パケット交換網を、エンド・ユーザに提供することである。もう１つの目的は、ＭＡＣのハンドオフ・メッセージをネットワークのハンドオフ・メッセージと統合化することである。さらに、本発明のもう１つの目的は、登録機能を、登録サーバに対して別に振り向け、そしてルーティング機能をインターワーキング機能ユニットに対して別々に振り向けることである。さらにもう１つの目的は、フォーリン・ネットワークの中の無線ハブ（アクセス・ハブＡＨとも呼ばれる）と、インターワーキング機能ユニット（ＩＷＦユニット）との間に中間のＸＴｕｎｎｅｌチャネルを提供することである。さらに、もう１つの目的は、フォーリン・ネットワークの中のインターワーキング機能ユニットとホーム・ネットワークの中のインターワーキング機能との間にＩＸＴｕｎｎｅｌチャネルを提供することである。さらにもう１つの目的は、モバイルのエンド・システムをサポートするためにレイヤ２のトンネリング・プロトコル（Ｌ２ＴＰ）を高度化することである。さらにもう１つの目的は、ＰＰＰ通信セッションを開始する前に、ネットワーク層の登録を実行することである。

【０００９】本発明の１つの実施形態によると、ピア・ツー・ピア・プロトコル・サーバによる通信を提供する無線データ・ネットワークが開示される。このネットワークは、ホーム移動交換センター、無線モデムおよび１つまたはそれ以上のエンド・システムを含む。その無線モデムとエンド・システムはイーサネット・リンクを経由して互いに接続されている。また、このネットワークはＰＰＰサーバをも含み、ＰＰＰサーバからエンド・システムに対して送信されるＰＰＰ情報は、イーサネット・フレームの中に無線モデムによってカプセル化され、イーサネット・リンク経由でエンド・システムに対して送信される。本システムは、図面を参照しながら、好適な実施形態についての以下の記述において詳細に説明される。

【００１０】

【発明の詳細な記述】本発明は、高速のパケット交換型の無線データ・リンク上で、バーチャル・プライベート・ネットワーク・サービスを使って、インターネットお

よびプライベート・イントラネットに対するリモート・アクセスをコンピュータ・ユーザに提供する。これらのユーザは無線リンク上でパブリック・インターネット、プライベート・イントラネットおよびそれぞれのインターネット・サービス・プロバイダに対してアクセスすることができる。そのネットワークはローミング、すなわち、現在のシステムによって提供されているサービスが利用できる任意の場所から、バーチャル・プライベート・ネットワーク・サービスを使ってインターネットおよびプライベート・イントラネットにアクセスするための機能をサポートする。また、そのネットワークはハンドオフ、すなわち、ＰＰＰクライアントとＰＰＰサーバとの間のＰＰＰリンクを乱すことなしに、ネットワークに対するユーザの付加のポイントを変更する機能をもサポートする。そのネットワークはホリゾンタル・インターネットおよびイントラネットのアプリケーションを実行しているユーザをターゲットとする。これらのアプリケーションとしては、電子メール、ファイル転送、ブラウザ・ベースのWWWアクセス、およびイントラネットの回りに構築されている他のビジネス・アプリケーションなどがある。そのネットワークはＩＥＴＦ標準に基づくことになるので、ＲＴＰなどのストリーミング・メディア・プロトコルおよびその上でのH．３２３などの会議プロトコルを実行することができる。

【００１１】他のインターネット・リモート・アクセス技術のうちで、既に配備されているもの、あるいは配備の各種の段階にあるものとしては、ＰＯＴＳおよびＩＳＤＮ、ＸＤＳＬのアクセスに基づいている無線回線のダイヤルアップ・アクセス、ＧＳＭ／ＣＤＭＡ／ＴＤＭＡに基づいている無線回路交換型アクセス、ＧＳＭ／ＣＤＭＡ／ＴＤＭＡに基づいている無線パケット交換型アクセス、ケーブル・モデムおよび衛星ベースのシステムなどがある。しかし、本発明のシステムは低い配備コスト、メンテナンスの容易性、広いフィーチャ・セット、スケーラビリティ、負荷の重い状態において洗練された方法で性能を劣化させる機能および、バーチャル・プライベート・ネットワーキング、ローミング、モビリティ、およびユーザおよびサービス・プロバイダの関連の利点に対するサービスの品質などのネットワーク・サービスの高度化に対するサポートを提供する。

【００１２】個人通信システム（ＰＣＳ）スペクトルを所有している無線サービス・プロバイダのために、本発明はＰＳＴＮを所有して稼働させている従来の有線回線のｔｅｌｃｏｓによって提供されるサービスと競合することができる、無線パケット交換データ・アクセス・サービスを提供できるようにする。また、無線サービス・プロバイダは自分自身がインターネット・サービス・プロバイダとなることを決定することができ、その場合、サービス・プロバイダはネットワーク全体を所有して稼働させることになり、ユーザに対してエンド・ツー・エンドのサービスを提供する。

【００１３】インターネット・サービス・プロバイダのために、本システムはインターネット・サービス・プロバイダがｔｅｌｃｏｓをバイパスすることができるようにし（それらのプロバイダがそのスペクトルを購入するか、あるいはリースする場合）、そして直接のエンド・ツー・エンドのサービスをユーザに提供し、おそらくｔｅｌｃｏｓに対するアクセス料金を節約できるようにする。そのサービスはインターネットが現在よりさらに大きくなるにつれて、将来において増加する可能性がある。

【００１４】本発明のシステムは柔軟性があり、インターネット・サービス・プロバイダではなく、ＩＳＰ、インターネットまたはプライベート・イントラネット・アクセスをエンド・ユーザに対して提供するだけである無線サービス・プロバイダにとって有利となる可能性がある。また、このシステムは無線アクセスおよびインターネット・サービスをエンド・ユーザに対して提供するサービス・プロバイダにも恩恵をもたらす可能性がある。また、このシステムは、無線アクセスおよびインターネット・サービスを提供するサービス・プロバイダにも恩恵をもたらすことができるが、そのネットワークの無線の部分が他のＩＳＰまたはプライベート・イントラネットに対するアクセスのために使われるようにすることができる。

【００１５】図２において、エンド・システム３２（たとえば、Ｗｉｎ　９５のパーソナル・コンピュータに基づいたシステム）は外付けまたは内蔵のモデムを使って無線ネットワーク３０に対して接続する。これらのモデムによってエンド・システムは媒体アクセス制御（ＭＡＣ）のフレームをエア・リンク３４上で送信および受信することができる。外付けのモデムは有線または無線のリンクを経由してＰＣに付加される。外付けのモデムは固定であり、そしてたとえば、ルーフ・トップ・マウントの指向性アンテナと同じ場所に設置される。外付けのモデムは８０２．３、汎用シリアル・バス、パラレル・ポート、赤外線、またはＩＳＭ無線リンクなどの手段のうちの１つを使って、ユーザのＰＣに対して接続することができる。内蔵モデムはラップトップのためのＰＣＭＣＩＡカードであることが好ましく、ラップトップのバックプレーンにプラグインされる。小型の全方向性アンテナを使って、それらはＭＡＣフレームをエア・リンク上で送信および受信する。また、エンド・システムも指向性アンテナを備えたラップトップ、ＡＣ電源線経由で接続されている指向性アンテナを備えた家庭における固定型の無線局などであってもよい。

【００１６】広域の無線カバレージが基地局３６によって提供される。基地局３６は１９９７年１２月２６日出願の米国特許出願第０８／９９８，５０５号に記述されているような５チャネルの再使用通信方式を採用するこ

とができる。基地局３６によって提供されるカバレージの範囲は、リンクの予算、容量およびカバレージなどのファクタによって変わる。基地局は、通常は、ＰＣＳ（個人通信サービス）無線サービス・プロバイダによってセル・サイトに設置される。基地局はそれぞれのカバレージ領域から、そのシステムの移動交換センター（ＭＳＣ）４０に対するエンド・システムのトラヒックを、有線回線またはマイクロ波バックホール（ｂａｃｋｈａｕｌ）（逆送）ネットワーク３８上でマルチプレックスする。

【００１７】そのシステムはエア・リンクのＭＡＣおよびＰＨＹ（物理）層およびモデムのタイプとは無関係である。またそのアーキテクチャも物理層およびバックホール・ネットワーク３８のトポロジーとは無関係である。バックホール・ネットワークのための唯一の条件は、基地局とＭＳＣとの間でインターネット・プロトコル（ＩＰ）パケットを十分な性能で回送することができなければならないということである。移動交換センター４０（ＭＳＣ４０）において、パケット・データ・インターワーキング機能（ＩＷＦ）５２が、このネットワークに対する無線プロトコルをターミネートする。ＩＰルータ４２はＭＳＣ４０をパブリック・インターネット４４、プライベート・イントラネット４６またはインターネット・サービス・プロバイダ４６に対して接続する。ＭＳＣ４０の中のアカウンティングおよびディレクトリ・サービス４８はアカウンティング・データおよびディレクトリ情報を格納する。要素管理サーバ５０は基地局、ＩＷＦおよびアカウンティング／ディレクトリ・サーバを含む機器を管理する。

【００１８】アカウンティング・サーバはユーザの代わりにアカウンティング・データを収集し、そのデータをサービス・プロバイダの料金請求システムに対して送信する。アカウンティング・サーバによってサポートされるインターフェースは、米国マネジメント協会（ＡＭＡ）のビリング・レコード・フォーマット、あるいは任意の他の適切なビリング・フォーマットで、ＴＣＰ／ＩＰ（トランスポート制御プロトコル／インターネット・プロトコル）トランスポート上で料金請求システム（図示せず）に対してアカウンティング情報を送信する。

【００１９】ネットワークのインフラストラクチャがＰＰＰ（ポイント・ツー・ポイント・プロトコル）サービスをエンド・システムに対して提供する。そのネットワークは、（１）エンド・システムに対するローミング（その無線のカバレージが利用できるどこにでもログ・インする）による固定の無線アクセスおよび、（２）低速のモビリティおよびハンドオフを提供する。エンド・システムがネットワークにログ・オンするとき、固定型のサービス（すなわち、静止的であって、ハンドオフ・サービスを必要としないサービス）またはモバイル・サービス（すなわち、ハンドオフ・サービスを必要とする

サービス）を要求することができる。固定型か、モバイルかを指定しないエンド・システムは、モバイル・サービスを指定しているとみなされる。そのエンド・システムの実際の登録は、サービスの要求されているレベル、そのエンド・システムのユーザによって申し込れたサービスのレベル、およびネットワークの中で利用できるファシリティに基づいたホーム登録サーバとのネゴシエーションの結果である。

【００２０】そのエンド・システムが固定型のサービス登録（すなわち、ハンドオフ・サービスを必要としない）をネゴシエートし、そのエンド・システムがホーム・ネットワークにある場合、ＩＷＦ（インターワーキング機能）が、そのエンド・ユーザとＰＰＰサーバなどの通信サーバ（すなわち、パブリック・インターネットに対する直接のアクセスを顧客に提供するために無線サービス・プロバイダによって稼働されているＩＳＰ　ＰＰＰサーバまたは企業のイントラネットＰＰＰサーバなどの接続されるべきポイント）との間でトラヒックを中継するためにその基地局に実装されている。メッセージ・トラヒックのおそらく８０％がこのカテゴリーのものであることが予想され、したがって、このアーキテクチャはＩＷＦ処理を基地局に分配し、中央の移動交換センターにおけるトラヒックの混雑を避ける。

【００２１】エンド・システムがモバイル・サービスを要求する場合（ホーム・ネットワークまたはフォーリン・ネットワークから）、あるいはエンド・システムがローミング・サービス（すなわち、フォーリン・ネットワークを通してのホーム・ネットワークからのサービス）を要求する場合、２つのＩＷＦが設立される。それらはそのエンド・システムが付加されているネットワーク（ホーム・ネットワークあるいはフォーリン・ネットワークのいずれであっても）の基地局に通常は設立されるサービスしているＩＷＦ、および、通常は、ホーム・ネットワークの移動交換センターＭＳＣに設立されるホームＩＷＦである。この状況はメッセージ・トラヒックの約２０％だけしか必要としないことが予想されるので、移動交換センターの回りのメッセージ・トラヒックの混雑は最小化される。サービスしているＩＷＦおよび無線ハブは同じネストのコンピュータに共存させること、あるいは同じコンピュータにプログラムすることさえもでき、それによって、ＸＴｕｎｎｅｌのプロトコルを使っているトンネルが無線ハブとサービスしているＩＷＦとの間に設立される必要はない。

【００２２】しかし、利用できるファシリティおよび要求されているサービスのタイプおよび品質に基づいて、フォーリンＭＳＣの中のファシリティから１つのフォーリン・ネットワークの中のサービスしているＩＷＦを代わりに選定することができる。一般に、ホームＩＷＦは通信セッションの間に変更されないアンカー・ポイントとなるが、サービスしているＩＷＦはエンド・システム

が十分に大きく移動する場合、変化する可能性がある。

【００２３】基地局は１つのアクセス・ハブおよび少なくとも１つのアクセス・ポイント（それがリモートにあっても、あるいはそのアクセス・ハブと同じ場所にあっても）を含む。通常、アクセス・ハブは複数のアクセス・ポイントにサービスする。エンド・システムは本発明の内容に従って、有線またはケーブルによってアクセス・ポイントに付加することができるが、１つの好適な実施形態においては、エンド・システムは無線の「エア・リンク」によってアクセス・ポイントに付加され、その場合、そのアクセス・ハブは便宜的に無線ハブと呼ばれる。この説明全体を通じてアクセス・ハブは「無線ハブ」と呼ばれるが、有線またはケーブルによって１つのアクセス・ハブに対して１つのアクセス・ポイントを通じて結合されるエンド・システムは等価の実装であり、「アクセス・ハブ」という用語によって考慮されることを理解されたい。

【００２４】本発明においては、エンド・システムはエンド・ユーザ登録エージェント（たとえば、そのエンド・システムのコンピュータ上で実行されるソフトウェア、そのモデムまたはその両方）を含み、そのエージェントはアクセス・ポイントと通信し、そしてそのアクセス・ポイントを通じて無線ハブに対して通信する。無線ハブはエンド・ユーザの登録エージェントに対する代行者として働いているプロキシ（代行）登録エージェント（たとえば、その無線ハブの中のプロセッサ上で実行されているソフトウェア）を含む。たとえば、ＩＥＴＦ提案のモバイルＩＰ標準において使われている概念は、一般にフォーリン・エージェント（ＦＡ）と呼ばれる。この理由のために、本発明のシステムのプロキシ登録エージェントはフォーリン・エージェントと呼ばれ、そしてモバイルＩＰのフォーリン・エージェントとは異なる本発明のシステムのフォーリン・エージェントの態様が、次の説明全体を通じて記述される。

【００２５】基地局の中のプロキシ登録エージェント（すなわち、フォーリン・エージェントＦＡ）を使って、エンド・システムのユーザ登録エージェントはそのネットワークに対する付加のポイントを発見することができ、そしてそのホーム・ネットワークのＭＳＣ（移動交換センター）の中の登録サーバによって登録することができる。そのホーム登録サーバはそのネットワークの中の複数のインターワーキング機能モジュール（ＩＷＦ）（実際には、ＭＳＣおよび無線ハブの両方においてプロセッサ上で実行されるソフトウェア・モジュール）のそれぞれの利用可能性を判定し、登録されたエンド・システムに対してＩＷＦを割り当てる。登録された各エンド・システムに対して、１つのトンネル（ＸＴｕｎｎｅｌプロトコルを使っている）が基地局の中の無線ハブと移動交換センター（ＭＳＣ）の中のインターワーキング機能（ＩＷＦ）との間に生成され、このトンネルがエンド・システムとＩＷＦとの間でＰＰＰフレームを転送する。

【００２６】ここで使われているように、ＸＴｕｎｎｅｌのプロトコルはフロー制御によってＰＰＰデータ・フレームのイン・シーケンスの転送でを提供するプロトコルである。このプロトコルは標準のＩＰネットワーク上、あるいはポイント・ツー・ポイントのネットワーク上、あるいは、ＡＴＭデータ・ネットワークまたはフレーム・リレー・データ・ネットワークのような交換ネットワーク上で実行することができる。そのようなネットワークはＴ１またはＴ３のリンクに基づくことができ、あるいは地上ベース、あるいは空間ベースのいずれであっても、無線リンクに基づくことができる。ＸＴｕｎｎｅｌのプロトコルはＬ２ＴＰ（レベル２のトランスポート・プロトコル）からのアルゴリズムを適応させることによって構築することができる。データ・パケットの消失が発生する可能性のあるリンクに基づいているネットワークにおいては、再送信の機能を選択できることが望ましいオプションである。

【００２７】エンド・システムのＰＰＰピア（すなわち、通信サーバ）はＩＷＦの中、あるいは企業のイントラネットまたはＩＳＰのネットワークに駐在することができる。ＰＰＰピアがＩＷＦに駐在しているとき、エンド・システムには直接のインターネット・アクセスが提供される。ＰＰＰピアがイントラネットまたはＩＳＰに駐在しているとき、エンド・システムにはイントラネットのアクセスまたはＩＳＰに対するアクセスが提供される。イントラネットまたはＩＳＰのアクセスをサポートするために、ＩＷＦはレイヤ２のトンネリング・プロトコル（Ｌ２ＴＰ）を使ってイントラネットまたはＩＳＰのＰＰＰサーバに接続する。イントラネットＩＳＰのＰＰＰサーバの観点からは、ＩＷＦはネットワーク・アクセス・サーバ（ＮＡＳ）のように見える。エンド・システムとＩＷＦとの間のＰＰＰトラヒックは基地局の中のフォーリン・エージェントによって中継される。

【００２８】逆の（アップ・リンクの）方向においては、エンド・システムからＩＷＦに対して転送されるＰＰＰフレームは、ＭＡＣおよびエア・リンク上で基地局に対して送られる。基地局はＸＴｕｎｎｅｌプロトコルを使って、ＭＳＣの中のＩＷＦに対してこれらのフレームを中継する。ＩＷＦはそれらを処理のためにＰＰＰサーバへ配送する。インターネット・アクセスの場合、ＰＰＰサーバをＩＷＦと同じマシンに置くことができる。ＩＳＰまたはイントラネット・アクセスの場合、ＰＰＰサーバはプライベート・ネットワークにあり、そしてＩＷＦはレイヤ２のトンネリング・プロトコル（Ｌ２ＴＰ）を使ってそれに接続する。順方向（ダウン・リンク）においては、ＰＰＰサーバからのＰＰＰフレームはＸＴｕｎｎｅｌプロトコルを使って、基地局に対してＩＷＦによって中継される。基地局はダウン・リンク・フ

レームをトンネルから取り出し、それらをエア・リンク上にエンド・システムに対して中継し、そこでそれらはエンド・システムのＰＰＰ層によって処理される。

【００２９】モビリティをサポートするために、ハンドオフに対するサポートが含まれている。ＭＡＣ層は基地局およびエンド・システムの中のモビリティ管理ソフトウェアがハンドオフの効率的な実行を支援する。ハンドオフはピアのＰＰＰエンティティおよびＬ２ＴＰトンネルには気付かれずに（トランスペアレントに）処理される。エンド・システムが１つの基地局から別の基地局へ移動する場合、その新しい基地局と元のＩＷＦとの間に新しいＸＴｕｎｎｅｌが生成される。前の基地局からの前のＸＴｕｎｎｅｌは削除される。ＰＰＰフレームはその新しい経路をトランスペアレントに通過することになる。

【００３０】そのネットワークはローミングをサポートする（すなわち、エンド・ユーザがフォーリンの無線サービス・プロバイダを通じてホームの無線サービス・プロバイダに接続するとき）。この機能を使ってエンド・システムはそのホーム・ネットワークから離れてフォーリン・ネットワークへロームし、しかもサービスを得ることができる。ただし、もちろん、そのフォーリン無線サービス・プロバイダとそのエンド・システムのホーム無線サービス・プロバイダがサービス契約を結んでいる場合である。

【００３１】図３において、ロームしているエンド・システム６０はフォーリン無線サービス・プロバイダ６２がカバレージを提供している場所までやって来ている。しかし、ロームしているエンド・システム６０はホームの無線サービス・プロバイダ７０と加入者の関係がある。本発明においては、ホームの無線サービス・プロバイダ７０はフォーリンの無線サービス・プロバイダ６２と契約関係にあってアクセス・サービスを提供する。したがって、ロームしているエンド・システム６０はエア・リンク上でフォーリンの無線サービス・プロバイダ６２の基地局６４に接続する。その時、データはロームしているエンド・システム６０から基地局６４を通じてフォーリンの無線サービス・プロバイダ６２のサービスしているＩＷＦ６６を通じてホームの無線サービス・プロバイダ７０のホームＩＷＦ７２に対して中継され、あるいはホームの無線サービス・プロバイダ７０のホームＩＷＦ７２を通じてインターネット・サービス・プロバイダ７４に対して中継されることも可能である。

【００３２】Ｉインターフェースと呼ばれているサービス・プロバイダ間のインターフェースが、ローミングをサポートするために、無線サービス・プロバイダ（ＷＳＰ）の境界に渡っての通信のために使われる。このインターフェースはフォーリンのＷＳＰとホームのＷＳＰとの間でエンド・システムのＰＰＰフレームを認証し、登録するため、および転送するために使われる。

【００３３】アップ・リンク方向およびダウン・リンク方向のＰＰＰフレームは、エンド・システムのホーム無線プロバイダ（ＷＳＰ）を通して転送される。代わりに、ＰＰＰフレームはフォーリンＷＳＰからデスティネーション・ネットワークへ直接転送される。フォーリンのＷＳＰの中の基地局はそのフォーリン・ネットワークの中でエンド・システムが付加されるポイントである。この基地局はＰＰＰフレームをフォーリンのＷＳＰの移動交換センターの中のサービスしているＩＷＦに対して送信する（また、ＰＰＰフレームをフォーリンのＷＳＰの移動交換センターの中のサービスしているＩＷＦから受信する）。サービスしているＩＷＦは両方向でエンド・システムのＰＰＰフレームを転送するために、レイヤ２のトンネルを使ってホームＩＷＦに対してＩインターフェース上で接続する。フォーリンのＷＳＰの中のサービスしているＩＷＦは監査のためのアカウンティング・データを収集する。ホームのＷＳＰの中のホームＩＷＦは料金請求のためのアカウンティング・データを収集する。

【００３４】フォーリンのＷＳＰの中のサービスしているＩＷＦを同じシステム内の基地局と組み合わせ、それによってＸＴｕｎｎｅｌを不要にすることができる。

【００３５】登録フェーズの間に、フォーリンのＷＳＰの中の登録サーバは、ロームしているエンド・システムのホーム・ネットワークのアイデンティティを知る。この情報を使って、フォーリン登録サーバはホーム登録サーバと通信し、そのエンド・システムを認証し、登録する。これらの登録メッセージはＩインターフェース上を流れる。エンド・システムが認証されて登録されると、レイヤ２のトンネルがＸＴＵＮＮＥＬのプロトコルを使って、その基地局とそのサービスしているＩＷＦとの間に生成され、そしてもう１つのレイヤ２のトンネルがＩインターフェース上でサービスしているＩＷＦとホームＩＷＦとの間に生成される。ホームＩＷＦはＬ２ＴＰ（レベル２のトンネル・プロトコル）を使って、前と同様にエンド・システムのＰＰＰピアに接続する。ハンドオフの間に、ホームＩＷＦとＬ２ＴＰのトンネルのロケーションは固定されたままになっている。エンド・システムが１つの基地局から別の基地局へ移動する際に、新しいトンネルが、その新しい基地局とサービスしているＩＷＦとの間に生成され、前の基地局とサービスしているＩＷＦとの間の前のトンネルは削除される。エンド・システムが十分に遠くへ移動し、したがって、新しいサービスしているＩＷＦが必要である場合、新しいトンネルがその新しいサービスしているＩＷＦとホームＩＷＦとの間に生成されることになる。前のサービスしているＩＷＦとホームＩＷＦとの間の前のトンネルは削除される。

【００３６】ローミングをサポートするために、Ｉインターフェースは無線サービス・プロバイダの境界にまた

がる認証、登録およびデータ転送をサポートする。認証および登録のサービスはＩＥＴＦのＲａｄｉｕｓのプロトコルを使ってサポートされる。レイヤ２のトンネル上でＰＰＰフレームを転送するためのデータ転送サービスは、Ｉ－ＸＴｕｎｎｅｌプロトコルを使ってサポートされる。このプロトコルはＩＥＴＦのＬ２ＴＰプロトコルに基づいている。

【００３７】この説明において使われたように、ホームＩＷＦはエンド・システムのホーム・ネットワークの中のＩＷＦを指す。サービスしているＩＷＦという用語は、エンド・システムに対して一時的にサービスを提供しているフォーリン・ネットワークの中のＩＷＦを指す。同様に、ホーム登録サーバという用語はそのエンド・システムのホーム・ネットワークの中の登録サーバを指し、フォーリン登録サーバという用語はフォーリン・ネットワークの中の登録サーバを指し、そこを通じてエンド・システムがローミング中に登録する。

【００３８】ネットワークはエンド・システムに対する固定の、および動的なＩＰアドレス割り当ての両方をサポートする。考慮される必要があるＩＰアドレスのタイプが２つある。第１のタイプはエンド・システムのそのホーム・ネットワーク内でのアイデンティティである。これはｕｓｅｒ＠ｄｏｍａｉｎというフォーマットの中で構造化されているユーザ名であってよい。これはモバイルＩＰの中で使われているホームＩＰアドレスとは異なっている。第２のアドレスはＰＰＰのＩＰＣＰアドレスのネゴシエーション・プロセスを経由してエンド・システムに対して割り当てられるＩＰアドレスである。ホーム・アドレスのドメインのサブフィールドがそのユーザのホーム・ドメインを識別するために使われ、そしてそれは完全にクオリファイされたドメイン名である。そのホーム・アドレスのｕｓｅｒのサブフィールドはそのホーム・ドメインの中でのユーザを識別するために使われる。ユーザ名（Ｕｓｅｒ－Ｎａｍｅ）はそのエンド・システム上およびＭＳＣにおける加入者データベースに格納されており、そしてユーザがそのサービスに加入するときにそのユーザに対して割り当てられる。ユーザ名のドメイン・サブフィールドは登録および認証の目的のため、ローミングの関係およびホーム登録サーバを識別するためにローミング中に使われる。構造化されたユーザ名の代わりに、別のユニークな識別子を使ってそのユーザのホーム・ネットワークおよびそのユーザのホーム・ネットワーク内でのアイデンティティを識別することができる。この識別子はエンド・システムによって登録要求の中で送られる。

【００３９】ＰＰＰ　ＩＰＣＰはエンド・システムに対するＩＰアドレスをネゴシエートするために使われる。ＩＰのコンフィギュレーション・プロトコルＩＰＣＰを使って、エンド・システムは固定の、あるいは動的なＩＰアドレスをネゴシエートすることができる。

【００４０】ホーム・アドレスとして構造化されたユーザ名フィールドを使い、そしてＩＰアドレスを使わないことが、既知のモバイルＩＰ上で本発明のシステムを特徴付ける機能であるが、モバイルＩＰおよび、ＰＰＰのエンド・システムに関するその使用が一般的になってくる場合に、ユーザ名がなく、ヌルでないホーム・アドレスだけを有するエンド・システムをサポートするようにもネットワークを機能強化することができる。ＰＰＰサーバはＩＰＣＰのアドレス割り当てフェーズの間にそのエンド・システムのホームＩＰアドレスと同じＩＰアドレスを割り当てるようにサービス・プロバイダによって構成することができる。この場合、ホーム・アドレスとＩＰＣＰによって割り当てられたＩＰアドレスとは同じになる。

【００４１】図４において、基地局６４およびエンド・システムからのエア・リンクが無線のサブネットワーク８０を形成し、それはエンド・ユーザのアクセスのためのエア・リンク、少なくとも１つの基地局（たとえば、基地局６４）およびその基地局からＭＳＣ４０（図２）への少なくとも１つのバックホール・ネットワーク（たとえば、図２の３８）を含む。たとえば、３セクター型の基地局の無線サブネットワークのアーキテクチャは次の論理機能を含む。

【００４２】１．アクセス・ポイント機能。アクセス・ポイント８２はＭＡＣ層のブリッジングおよびＭＡＣ層の関連付けおよび関連付け解除の手順を実行する。アクセス・ポイントは１つのプロセッサ（カスタムのアプリケーション固有の集積回路（ＡＳＩＣ）の形が好ましい）、無線ハブに対するリンク（カード上のイーサネット・リンクまたはＡＳＩＣに組み込まれている形式が好ましい）、アンテナに対するリンク（データ変調器／復調器および送信機および受信機を備えたカードの形式であることが好ましい）、およびそのエンド・システムが結合されているアンテナを含む。そのプロセッサはデータのブリッジング機能および、以下にさらに説明されるような登録およびモビリティのハンドオーバをサポートする各種の他の機能を行うためのソフトウェアを実行する。図７、図８および図１１に関する説明を参照されたい。アクセス・ポイント（ＡＰ）はＭＡＣ層のフレームをエア・リンクから取り、それらを無線ハブに対して中継し、また、その逆を行う。ＭＡＣ層の関連付けおよび関連付け解除の手順がＡＰによって使われ、ＡＰはそれぞれのアドレス・フィルタ・テーブルにエンド・システムのＭＡＣアドレスのリストを維持する。ＡＰはＭＡＣアドレスがそのテーブルに存在しているエンド・システムに代わって単にＭＡＣ層のブリッジングを行うだけである。アクセス・ポイントおよびその関連付けられている無線ハブは、通常は同じ場所に設置されている。その最も単純な形式においては、アクセス・ポイントは無線ハブに対する１つのポートに過ぎない。ＡＰと無線ハブ

が同じセル・サイトに共存しているとき、それらをＩＥＥＥ　８０２．３のリンク経由で一緒に接続することができる。アクセス・ポイントが無線ハブから離れた場所にあって有線のＴ１幹線、または場合によっては無線幹線などの長距離リンクを経由して接続されていることが時々ある。多重セクターのセルの場合、複数のアクセス・ポイント（すなわち、セクター当たりに１つ）が使われる。

【００４３】２．無線ハブの機能。無線ハブ８４はフォーリン・エージェント（ＦＡ）の手順、バックホールの負荷バランシング（たとえば、複数のＴ１上での）、バックホール・ネットワークのインターフェーシング、およびｘｔｕｎｎｅｌの手順を実行する。サービスの品質（ＱＯＳ）に対するサポートがあるとき、無線ハブはｘｔｕｎｎｅｌのプロトコルを、ＱＯＳ属性が異なっているバックホール上で実行することによってＱＯＳに対するサポートを実施する。多重セクター・セルのサイトにおいては、単独の無線ハブ機能が複数のアクセス・ポイントによって共有されるのが普通である。無線ハブは１つのプロセッサ、１つまたはそれ以上のアクセス・ポイントに対する１つのリンク（カード上でのイーサネット・リンクの形式またはＡＳＩＣに組み込まれている形式が好ましい）、およびバックホール回線に対する１つのリンクを含む。バックホール回線は、通常は、Ｔ１またはＴ３通信回線であり、それは無線サービス・プロバイダの移動交換センターにおいてターミネートしている。バックホール回線に対するリンクはデータを好ましいフォーマット、たとえば、イーサネット・フォーマット、フレーム・リレーのフォーマット、またはＡＴＭのフォーマットにフォーマット化する。無線ハブのプロセッサはデータのブリッジングおよび、ここに説明されているような各種の他の機能をサポートするためのソフトウェアを実行する。図９、図１０および図１１に関する説明を参照されたい。

【００４４】基地局の設計は次のタイプのセル・アーキテクチャをサポートする。

１．ローカルＡＰアーキテクチャ。ローカルＡＰアーキテクチャにおいては、アクセス・ポイントの範囲は大きい（通常、＞＝２ｋｍ）。それらのアクセス・ポイントは無線ハブと一緒にそのセル・サイトに共存している（図４）。アクセス・ポイントはＩＥＥＥ　８０２．３のネットワークを使ってその無線ハブに接続することができ、あるいはその無線ハブのバックプレーンに直接プラグインすることができ、あるいはいくつかの他のメカニズム（たとえば、汎用シリアル・バス、プリンタ・ポート、赤外線など）を使って無線ハブに接続することができる。最初の選択肢がこの説明の残りの部分に対して使われることが仮定される。そのセル・サイトは無線ハブに対して複数のアクセス・ポイントおよびセクター型のアンテナを追加することによって、乗合いの、あるいはセクター型のサイトとすることができる。

【００４５】２．リモートのＡＰアーキテクチャ。リモートのＡＰアーキテクチャにおいては、アクセス・ポイントの範囲は非常に小さいのが普通であり、通常は、半径が約１ｋｍである。それらは無線ハブから離れた場所（室内または屋外）に設置される。無線が置かれているセル・サイトに対してリモートのアクセス・ポイントをリンクするのはＴ１幹線または無線幹線が好ましい。そのセル・サイトから、ＭＳＣの中のＩＷＦに接続するために、有線回線のバックホールまたはマイクロ波のリンクが通常使われる。リモートのＡＰと無線ハブとの間に無線幹線が使われる場合、幹線のために多目的の、またはセクター型の無線ラジオが利用される。リモートのアクセス・ポイントに対する幹線接続のための装置は無線ハブと同じ場所に設置されていることが好ましく、そしてＩＥＥＥ　８０２．３のネットワークを使ってそれに接続されるか、あるいはその無線ハブのバックプレーンに直接プラグインすることができる。これらの装置は幹線ＡＰという用語で呼ばれる。

【００４６】３．混合型のＡＰアーキテクチャ。混合型のアーキテクチャにおいては、無線のサブネットワークはリモートおよびローカルのアクセス・ポイントをサポートしなければならなくなる。リモートのアクセス・ポイントは穴埋めのため、および他の容量に関する理由のために追加される可能性がある。前に説明されたように、Ｔ１または無線の幹線を使ってリモートのＡＰを無線ハブに接続することができる。

【００４７】図５はローカルのＡＰだけを使っている３つのセクターを備えたセルを示している。アクセス・ポイントおよび無線ハブは基地局に共存しており、互いに８０２．３のリンクで接続されている。

【００４８】図６は無線幹線８６を使って無線ハブ８４に接続されているリモートのアクセス・ポイント８２によるアーキテクチャを示している。基地局の中の各幹線アクセス・ポイントはリモートのマイクロ・アクセス・ポイント（図中のＲ－ＡＰ）に対するポイント・ツー・マルチポイントの無線ラジオ・リンクにを提供する。そのリモートのアクセス・ポイントがエンド・システムに対するエア・リンクのサービスを提供する。無線ハブおよび幹線アクセス・ポイントは基地局に共存しており、そして８０２．３のリンクを経由して互いに接続されている。また、この図はポイント・ツー・ポイントのＴ１リンクを経由して無線ハブに対して接続されているリモートのアクセス・ポイントの８２Ｒをも示している。このシナリオにおいては、幹線ＡＰは不要である。

【００４９】上記のセル・アーキテクチャおよび各セルが使う可能性があるアクセス・ポイントの各種のタイプのすべてをサポートするために、ネットワーク・アーキテクチャは次の規則に従う。

１．アクセス・ポイントがＭＡＣ層のブリッジとして機

能する。リモートのアクセス・ポイントはエンド・システムに対するエア・リンクとセル・サイトに対する無線またはＴ１の幹線との間のＭＡＣブリッジングを実行する。ローカルのアクセス・ポイントはエンド・システムに対するエア・リンクと無線ハブとの間のＭＡＣブリッジングを実行する。

【００５０】２．幹線アクセス・ポイントもＭＡＣ層のブリッジとして機能する。それらは幹線（アクセス・ポイントに対して接続されている）と無線ハブとの間のＭＡＣブリッジングを実行する。

【００５１】３．無線ハブは最初に８０２．３のリンクを使って共存しているすべてのＭＡＣブリッジ（すなわち、ローカルのアクセス・ポイントまたは幹線アクセス・ポイント）に対して接続されている。

【００５２】さらに、Ｔ１幹線付きのローカル・アクセス・ポイントまたはリモートのアクセス・ポイントが使われている場合、次の規則に従う。

１．ローカルのアクセス・ポイントが無線ハブと同じ場所に設置され、ポイント・ツー・ポイントの８０２．３のリンクまたは共有型の８０２．３のネットワークを使ってそれに接続されている。リモートのアクセス・ポイントはポイント・ツー・ポイントのＴ１幹線を使って無線ハブに接続されている。

【００５３】２．セクター化はセクター型のアンテナを備えたアクセス・ポイントをセル・サイトに追加することによってサポートされる。

【００５４】３．無線ハブに接続されている各アクセス・ポイントに対して、エンド・システムの登録に参加する無線ハブの中で実行するフォーリン・エージェントがある。ＭＡＣ層の関連付けの手順がアクセス・ポイントのＭＡＣアドレスのフィルタ・テーブルを最新の状態に保つため、およびＭＡＣ層のブリッジングを効率的に実行するために使われる。無線ハブはＭＡＣの関連付け機能に参加し、有効なＭＡＣアドレスだけがアクセス・ポイントのＭＡＣアドレス・フィルタ・テーブルに追加されるようにする。

【００５５】４．無線ハブの中のフォーリン・エージェントはｘｔｕｎｎｅｌのプロトコルを使って、アクセス・ポイントとＭＡＣのＩＷＦとの間でフレームを中継する。ＭＡＣのアドレス・フィルタ・テーブルは、ＭＡＣアドレスがそのテーブルに存在しないユニキャストのＭＡＣデータ・フレームをフィルタ・アウトするために使われる。ＡＰは常にＭＡＣのブロードキャスト・フレームおよび、エンド・システムの登録機能に関連付けられているＭＡＣフレームを、ＭＡＣアドレス・フィルタ・テーブルの内容とな無関係に転送する。

【００５６】５．ローカルのアクセス・ポイントはＡＲＰを使って、ＩＰトラヒックを無線ハブに対して回送するためのＭＡＣアドレスを解決する。逆に、無線ハブはＩＰパケットをアクセス・ポイントに対して回送するためにもＡＲＰを使う。ＵＤＰ／ＩＰがアクセス・ポイントのネットワーク管理のために使われる。

【００５７】６．Ｔ１を経由して接続されているリモートのアクセス・ポイントはＡＲＰを使用しない。というのは、そのリンクはポイント・ツー・ポイントのリンクとなるからである。

【００５８】７．ハンドオフのためのサポートはＭＡＣ層からの支援によって行われる。

【００５９】無線幹線および幹線ＡＰを使っているセル・アーキテクチャにおいては、次の規則が守られる。

１．幹線のアクセス・ポイントは無線ハブと同じ場所に設置され、ポイント・ツー・ポイントの８０２．３のリンクまたは他の適切な手段を使ってそれに接続されている。

【００６０】２．無線幹線のセクター化はそのセル・サイトに対してセクター型のアンテナを備えている幹線アクセス・ポイントを追加することによってサポートされる。

【００６１】３．バックホール・セクターにまたがるハンドオフは無線ハブの中のフォーリン・エージェントを使って行われる。各バックホール・セクターに対して、無線ハブの中で実行しているフォーリン・エージェントが存在する。

【００６２】４．幹線ＡＰはＭＡＣ層のエンド・システムの関連付けおよびハンドオフの手続きには参加する必要はない。それぞれのＭＡＣアドレス・フィルタ・テーブルはエンド・システムがそのネットワークに登録する際に無線ハブによって動的にプログラムされる。ＭＡＣのアドレス・フィルタ・テーブルはＭＡＣフレームをフィルタ・アウトするために使われる。ブロードキャストのＭＡＣフレームまたは登録パケットを含んでいるＭＡＣフレームは、常に通過することが許される。

【００６３】５．幹線ＡＰはＡＲＰを使ってＩＰトラヒックを無線ハブに対して回送するためのＭＡＣアドレスを解決する。逆に、無線ハブはＡＲＰを使ってＩＰパケットを幹線ＡＰに対して回送する。ＵＤＰ／ＩＰが幹線ＡＰのネットワーク管理のために使われる。

【００６４】６．単独の無線幹線セクターにおいては、１つのアクセス・ポイントから別のアクセス・ポイントへのＭＡＣの関連付けおよびハンドオフは、無線ハブの中のフォーリン・エージェントの支援によってＭＡＣ層を使って行われる。これらのＭＡＣ層の手順を使って、エンド・システムはアクセス・ポイントに関係する。エンド・システムが１つのアクセス・ポイントから別のアクセス・ポイントへ移動する際、そのアクセス・ポイントはＭＡＣのハンド・オフ・プロトコルを使ってそれぞれのＭＡＣアドレス・フィルタ・テーブルを更新する。そのセル・サイトにある無線ハブはアクセス・ポイントがこの機能を実行するための支援を提供する。この支援は、ＭＡＣ層のハンド・オフ・メッセージの中継（アク

セス・ポイントはＭＡＣ層上で互いには直接通信することができないので）および、ＭＡＣ層の登録およびハンドオフのため、およびそのアクセス・ポイントのＭＡＣアドレス・フィルタ・テーブルの更新のためのエンド・システムの認証を含む。

【００６５】７．無線幹線セクターに対するフォーリン・エージェントはｘｔｕｎｎｅｌプロトコルを使って幹線ＡＰとＭＳＣとの間でのフレームの中継を担当する。したがって、幹線ＡＰに対するフォーリン・エージェントはその無線幹線セクター内でのアクセス・ポイントに関するエンド・システムのロケーションについては関係しない。ダウン・リンクの方向においては、それはそのトンネルから、そのバックホール・セクターに付加されているリモートのアクセス・ポイントのすべてに対してフレームを送信するために、ＭＡＣ層のブリッジングを使う適切な幹線ＡＰに対してフレームを転送するだけである。アクセス・ポイントはそれぞれのＭＡＣアドレス・フィルタ・テーブルを参照してそのＭＡＣフレームをアクセス・ネットワーク上で転送するか、あるいはそのＭＡＣフレームをドロップするかのいずれかを行う。上記のように、ＭＡＣアドレス・フィルタ・テーブルはＭＡＣ層の関連付けおよびハンドオフの手順を使って最新のものに保たれている。アップ・リンクの方向においては、ＭＡＣフレームはバックホール・ブリッジに対してアクセス・ポイントによって転送され、バックホール・ブリッジは８０２．３のリンクを使って無線ハブの中のフォーリン・エージェントに対してそれらを転送する。

【００６６】８．ＡＲＰはリモートのアクセス・ポイントに対するＩＰパケットの送信または受信には使われない。アクセス・ポイントはＢＯＯＴＰ手順を使って無線ハブのＭＡＣアドレスを決定する。逆に、無線ハブはリモートのアクセス・ポイントのＭＡＣアドレスによって構成される。ＵＤＰ／ＩＰがアクセス・ポイントのネットワーク管理のため、およびエンド・システムの関連付けおよびハンドオフのメッセージのために使われる。

【００６７】セル・サイトにおけるＩＥＥＥ標準８０２．３のリンクを他の速度のリンクによって置き換えることができる。

【００６８】図７はローカルのアクセス・ポイントに対するプロトコル・スタックを示している。そのスタックのベースには物理層ＰＨＹがある。物理層ＰＨＹは、一例として無線電波を使って空中でエンド・システムとの間でデータを搬送する。エンド・システムから受信したとき、ＡＰは物理層からデータを受信し、それをＭＡＣフレーム（ＭＡＣ層）からアンパックする。次に、エンド・システムのデータ・フレームはイーサネットの物理層のフォーマット（ＩＥＥＥ　８０２．３のフォーマット）に再パックされ、イーサネット・リンクを経由して無線ハブに対して送信される。そのＡＰのプロセッサがデータを無線ハブからそのイーサネット・リンク、すなわち、物理層経由で受信すると、そのデータはエンド・システムへ送信され、ＡＰはそのデータを媒体アクセス制御（ＭＡＣ）のフォーマットにパックし、そのＭＡＣ層のデータを、物理層を使ってエンド・システムに対して送信されるようにその変調器に対して送信する。

【００６９】図８においては、図７のエンド・システムとの間のＭＡＣおよびＰＨＹ層は、リモートのアクセス・ポイントに対するセル・サイトに対する幹線のためのＭＡＣおよびＰＨＹによって置き換えられる。詳しく言えば、Ｔ１幹線の場合、上位レベルのデータ・リンク制御プロトコル（ＨＤＬＣプロトコル）がＴ１上で使われることが好ましい。

【００７０】図９はバックホール回線とリモートのアクセス・ポイントに対する幹線とをブリッジする無線ハブの場合のプロトコル・スタックを示している。リモートのＡＰに対する幹線はリモートのアクセス・ポイント（イーサネットに接続されているアクセス・ポイントとは異なる）をサポートするためだけに必要である。リモートのＡＰに対する無線幹線のためのＭＡＣおよびＰＨＹ層はポイント・ツー・マルチポイントのリンクを提供し、１つの幹線が同じセクターの中の多くのリモートのＡＰと通信するために使われるようにする。

【００７１】無線ハブはリモートのＡＰおよびバックホール回線（たとえば、Ｔ１またはＴ３）に対する幹線を、そのネットワークの移動交換センター（ＭＳＣ）に対してブリッジする。無線ハブの中のプロトコル・スタックはＭＳＣに対するＭＡＣおよびＰＨＹの層を実装し、その層のトップにはＩＰ（インターネット・プロトコル）層が実装されており、ＩＰ層のトップにはネットワーク管理のためのＵＤＰ層（汎用データグラム・プロトコル（Ｕｎｉｖｅｒｓａｌ　ＤａｔａｇｒａｍＰｒｏｔｏｃａｌ）、組み合わせてＵＤＰ／ＩＰと呼ばれる）が実装され、ＵＤＰ層のトップにはＸＴｕｎｎｅｌのプロトコルが実装されている。そのＸＴｕｎｎｅｌのプロトコルは新しいフォーマットのプロトコルであり、そのフォーマットはモビリティの態様（たとえば、モバイルＩＰの中でのような）およびレベル２のトンネル・プロトコル（Ｌ２ＴＰ）の態様を含む。ＸＴｕｎｎｅｌのプロトコルは無線ハブからＭＳＣに対して通信するため、および異なるネットワークまたは同じネットワークの中のインターワーキング機能（ＩＷＦ）の間で使われる。

【００７２】図１０には、リモートのアクセス・ポイントをサポートするための基地局における中継機能に対するプロトコル・スタックが示されている。中継機能はバックホール回線に対するインターフェース（無線ハブとして示されている）およびリモートのＡＰ（幹線ＡＰとして示されている）に対するインターフェースを含む。無線ハブの観点からは、幹線ＡＰ（図７および図１０に示されている）は実際には図７に示されているＡＰと同様に動作する。基地局のプロトコル・スタックは無線の

ハブおよび、その間にイーサネットを備えた幹線ＡＰに分割されていることが好ましい。Ｎセクターの無線幹線においては、セル・サイトの中のＮ個の無線幹線ＡＰと１個の無線ハブがある。

【００７３】図１１には、ローカルＡＰを使っているセル・アーキテクチャのための基地局のプロトコル・スタックが示されている。中継機能は、バックホール回線（無線ハブとして示されている）に対するインターフェースおよび、エンド・システム（ＡＰとして示されている）に対するエア・リンク・インターフェースを含む。無線ハブの観点からは、ＡＰ（図８および図１１に示されている）は実際には図８に示されている幹線ＡＰと同様に動作する。基地局のプロトコル・スタックは無線ハブとその間のイーサネットでの幹線ＡＰに分割されている。Ｎセクターのセルの中には、Ｎ個のアクセス・ポイントおよび単独の無線ハブがある。

【００７４】基地局からＭＳＣへのバックホール・ネットワークは次の属性を有する。

１．そのネットワークは基地局とＭＳＣとの間でＩＰのデータグラムを回送することができる。

２．そのネットワークは安全である。それはパブリック・インターネットではない。信頼できるノードからのトラヒックだけがネットワーク上で許される。というのは、そのネットワークはエンド・システムのトラヒックを転送するだけでなく、認証の転送、アカウンティング、登録およびマネジメントのトラヒックに対しても使われるからである。

３．そのネットワークは必要な性能特性を備えている。

【００７５】代表的な応用においては、サービス・プロバイダは装置がインストールされるバックホール・ネットワークのインストールおよび維持を担当する。

【００７６】基地局はＭＳＣと通信するために次のバックホール・インターフェースをサポートする。

１．基地局はポイント・ツー・ポイントのＴ１または断片的Ｔ３リンクを使ってＨＤＬＣを備えたＰＰＰ上でのＩＰをサポートする。

２．基地局はＴ１または断片的Ｔ３リンクを使ってフレーム・リレー上でＩＰをサポートする。

３．基地局はＴ１または断片的Ｔ３リンクを使ってＡＡＬ５／ＡＴＭ上でＩＰをサポートする。

４．基地局はイーサネット・リンク上でＩＰをサポートする。

【００７７】上記のインターフェースのすべてがＩＥＴＦ標準のカプセル化に基づいているので、商用のルータをＭＳＣの中で使ってバックホール・ネットワークの物理リンクをターミネートすることができる。上位の層へは各種のサーバおよび他のプロセッサによって渡され、処理される。

【００７８】ＭＡＣ層の上でのエンド・システムの登録手順がサポートされる。次においては、ＭＡＣ層におけるエンド・システムの登録手順は、それらがその上の層に影響する場合を除いて無視される。

【００７９】エンド・システムはそれぞれのホーム・ネットワーク上で、あるいはフォーリン・ネットワークからサービスに対して登録することができる。両方のシナリオにおいて、エンド・システムはその基地局の中のフォーリン・エージェント（ＦＡ）を使って、そのネットワークに対する付加のポイントを発見し、そして登録する。前者の場合、ＦＡはそのエンド・システムのホーム・ネットワークの中にある。後者の場合、ＦＡはフォーリン・ネットワークの中にある。いずれの場合においても、そのネットワークはエンド・システムのホーム・ネットワーク内のＩＷＦをアンカー・ポイント（すなわち、移動性を無視してそのセッション全体を通じて不変である）として使う。エンド・システムとの間のＰＰＰフレームはその基地局の中のＦＡを経由してホーム・ネットワーク内のＩＷＦへ転送される。エンド・システムがホームにある場合、そのホームＩＷＦはその基地局に対するｘｔｕｎｎｅｌプロトコルの手段によって直接に接続される。ホームＩＷＦを同じノードの中の基地局と組み合わせることができることに留意されたい。エンド・システムがロームしている場合、フォーリン・ネットワークの中のサービスしているＩＷＦがＩインターフェース上でホームＩＷＦに対して接続されている。サービスしているＩＷＦは基地局とホームＩＷＦとの間でフレームを中継する。ホームＩＷＦを同じノードの中の基地局と組み合わせることができることを留意されたい。ホームＩＷＦから、同じＩＷＦの中に駐在することができるＰＰＰサーバに対して、あるいはＬ２ＴＰプロトコルを使っている別のサーバに対してデータが送信される。その別のサーバはその無線サービス・プロバイダとは異なるプライベート・ネットワーク・オペレータ（例えば、ＩＳＰまたは企業のイントラネット）によって所有され、そして運用されている可能性がある。そのセッションが続いている間、ホームＩＷＦとＰＰＰサーバのロケーションは固定されたままである。接続されている間にエンド・システムが移動した場合、それは新しいフォーリン・エージェントと再登録しなければならなくなる。しかし、同じホームＩＷＦおよびＰＰＰサーバが続けて使用される。新しいｘｔｕｎｎｅｌがその新しいＦＡとＩＷＦとの間に生成され、前のフォーリン・エージェントとそのＩＷＦとの間のｘｔｕｎｎｅｌは破棄される。

【００８０】図１２は２つのエンド・システムＡおよびＢに対するこのネットワーク構成を示している。それらは両方ともホーム無線ネットワークが無線サービス・プロバイダＡ（ＷＳＰ－Ａ）である。１つのエンド・システムがホーム無線ネットワークから登録され、そして他のエンド・システムはフォーリン無線ネットワークから登録される。ＷＳＰ－Ａの中のホームＩＷＦは両方のエ

ンド・システムに対するアンカー･ポイントとして働く。両方のエンド・システムに対して、データはホームＩＷＦに対して中継され、そのホームＩＷＦはＩＳＰ－Ａによって所有されているインターネット・サービス・プロバイダのＰＰＰサーバに対して接続される。ここで両方のエンド・システムが同じＩＳＰに加入していると仮定される。そうでない場合は、そのホームＩＷＦも別のＩＳＰに対して接続されるように示される。

【００８１】無線サービス・プロバイダのネットワーク内で、基地局とＩＷＦとの間のデータはｘｔｕｎｎｅｌプロトコルを使って搬送される。ＩＷＦとＰＰＰサーバとの間のデータはレベル２のトンネリング・プロトコル（Ｌ２ＴＰ）を使って搬送される。サービスしているＩＷＦとホームＩＷＦとの間のデータはＩ－ｘｔｕｎｎｅｌプロトコルを使って搬送される。

【００８２】単純なシナリオにおいては、固定型のサービスを要求しているそれぞれのホーム・ネットワークの中のユーザに対して、ホームＩＷＦの機能は基地局において動的に活性化することができる。また、サービスしているＩＷＦの機能を基地局の中でローミングしているユーザに対して活性化することができる。

【００８３】ホーム・ネットワークの中の１つのＩＷＦを常に使うことには、利点もあり、欠点もある。１つの明白な利点は、単純性である。１つの欠点はデータを場合によってはリモートのホームＩＷＦとの間で常に中継していなければならないことである。その代替案は必要なすべての情報をサービスしているＩＷＦへ送り、それがエンド・システムのＩＳＰ／イントラネットに対して接続できるようにし、そしてサービスしているＩＷＦに対してアカウンティング情報をほぼリアルタイムでホーム・ネットワークの中のアカウンティング・サーバに対して送り返すようにすることができる。この機能は実装が比較的複雑であるが、効率が良い。というのは、フォーリン・ネットワークからホーム・ネットワークへの、長い可能性のある距離にわたってデータを中継する必要性が減るからである。

【００８４】たとえば、シカゴから香港へロームするユーザの場合を考える。ユーザのホーム・ネットワークがシカゴにあって、そのユーザが香港にある無線サービス・プロバイダを使って登録する場合、最初の構成においては、アンカー・ポイントはシカゴにあるホームＩＷＦとなり、そしてすべてのデータが香港からシカゴへ、あるいはその逆に中継されなければならなくなる。シカゴにあるホームＩＷＦはシカゴにあるユーザのＩＳＰに接続する。第２の構成では、エンド・システムのユーザには香港にあるＩＳＰが割り当てられる。したがって、データは必ずしもシカゴと香港との間で往復して中継される必要はなくなる。この第２の構成においては、サービスしているＩＷＦはアンカーとして働き、そしてエンド・システムが移動した場合でもそのセッションの間中は

決して変化しない。しかし、ＦＡのロケーションは香港におけるエンド・システムの移動の結果として変化する可能性がある。

【００８５】図１３は第２のネットワーク構成を示している。この図の中で、エンド・システムＡおよびＢのホーム・ネットワークはＷＳＰ－Ａである。エンド・システムＡはそのホームＩＷＦをアンカー・ポイントとして使ってそのホーム・ネットワークから登録し、そしてＩＳＰのＰＰＰサーバを使ってそのＩＳＰ－Ａに対しても接続する。エンド・システムＢはＷＳＰ－Ｂのフォーリン・ネットワークから登録し、サービスしているＩＷＦを使用する。そのＩＷＦはアンカー・ポイントとして働き、そしてそのエンド・システムをＩＳＰに対して、そのＩＳＰのＰＰＰサーバを使って接続する。この構成においては、エンド・システムＢに対するデータはフォーリン・ネットワークからホーム・ネットワークに対して、およびその逆方向に中継される必要はない。

【００８６】この構成が正常に動作するためには、そのホームとフォーリンの無線サービス・プロバイダとの間にローミング契約がなければならないだけでなく、そのフォーリン無線サービス・プロバイダとエンド・システムのインターネット・サービス・プロバイダとの間にも、直接に、あるいは仲介者を通じて契約がなければならない。上記の例において、香港における無線サービス・プロバイダはシカゴにおける無線サービス・プロバイダと事業契約を結んでいなければならないばかりでなく、香港にあるＷＳＰもそのユーザのシカゴのＩＳＰと事業契約を結んでいなければならず、そして香港においてシカゴのＩＳＰのＰＰＰサーバに対してアクセスしなければならず、あるいは、そのユーザのシカゴのＩＳＰとローミングに対する事業契約を結んでいる香港におけるローカルな他のＩＳＰと事業契約を結んでいなければならない。さらに、香港にあるＷＳＰはユーザの認証およびアカウンティングを行うため、および適切なトンネルをセットアップするために、これらのローミングの関係を動的に発見することができなければならない。

【００８７】インターネットのインフラストラクチャ・ビジネスに参入している会社にとって、これらのシナリオのすべてに対してＩＥＴＦにおける適切な標準を正しく適用することは困難である。したがって、本発明のシステムにとって好ましい１つの実施形態は、ホーム・ネットワークの中のＩＷＦが常にアンカー・ポイントとして使われる、より単純な、やや効率的でない可能性がある構成を実装することである。しかし、インターネットのローミングに対する適切な業界標準のプロトコルの存在している中で、第２の構成は等価な、あるいは代替の実施形態とみなされるべきである。

【００８８】エンド・システムはそれがＰＰＰをスタートし、データを送信および受信することができる前に、無線ネットワークに登録しなければならなくなる。エン

ド・システムはまず最初にＦＡの発見および登録のフェーズを通る。これらのフェーズはそのエンド・システムを無線サービス・プロバイダに対して認証し、登録する。これらのフェーズが終了すると、エンド・システムはＰＰＰを開始する。これはＰＰＰリンクの確立のフェーズ、ＰＰＰの認証フェーズおよびＰＰＰネットワーク制御プロトコルのフェーズを含む。これらのフェーズが終わると、そのエンド・システムはＰＰＰを使ってＩＰパケットを送信および受信することができる。

【００８９】次の説明では、エンド・システムがフォーリン・ネットワークからロームし、そして登録していると仮定する。ＦＡの発見フェーズの間に、エンド・システムは（そのユーザ・ネゴシエーション・エージェントを通じて）フォーリン・エージェントからの公示を待つか、あるいは要請する。ユーザ登録エージェントは近くのフォーリン・エージェントから送られた公示メッセージを使ってそのＦＡのアイデンティティを発見し、そして登録する。このフェーズの間に、エンド・システムのユーザ登録エージェントは１つのＦＡを選択し、それに対して登録要求を発行する。プロキシ登録エージェントとして動作しているＦＡは、その登録要求をその登録サーバ（フォーリンＷＳＰの中の登録サーバ）に対して転送する。登録サーバはユーザの登録エージェントの要求からユーザ名を使ってそのエンド・システムのホーム・ネットワークを知り、そしてその登録要求を認証のためにホーム・ネットワークの中の登録サーバに対して転送する。フォーリン登録サーバによって中継された登録要求を受け取ると、ホーム登録サーバはそのフォーリン登録サーバのアイデンティティを認証し、また、そのエンド・システムのアイデンティティも認証する。認証および登録が成功した場合、そのホーム登録サーバはホーム・ネットワークの中で１つのＩＷＦを選択し、ホームＩＷＦと（フォーリンＷＳＰの中の）サービスしているＩＷＦとの間にＩ－ｘｔｕｎｎｅｌのリンクを生成する。ホーム・ネットワークの中のＩＷＦはそのＰＰＰセッションの間中、アンカー・ポイントとして働く。

【００９０】認証および登録のフェーズが終わると、各種のＰＰＰフェーズが開始される。ＰＰＰの開始時に、１つのＬ２ＴＰコネクションが、ホームＩＷＦと要求されたＩＳＰ／イントラネットＰＰＰサーバとの間に生成される。ＰＰＰの認証フェーズにおいて、パスワード認証プロトコル（ＰＡＰ）またはチャレンジ認証プロトコル（Ｃｈａｌｌｅｎｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）（ＣＨＡＰ）を使ってＰＰＰパスワードが交換され、ＩＳＰまたはイントラネットのＰＰＰサーバがそのエンド・システムのアイデンティティを独立に認証する。

【００９１】これが成功すると、ＰＰＰネットワーク制御フェーズが開始される。このフェーズにおいて、ＩＰアドレスがネゴシエートされ、ＰＰＰサーバによってエンド・システムに割り当てられ、そしてＴＣＰ／ＩＰヘッダの圧縮の仕様についてもネゴシエートされる。これが完了すると、そのエンド・システムはＰＰＰを使ってＩＰパケットをそのＩＳＰまたは企業のイントラネットとの間で送受信することができる。

【００９２】ここで、２レベルの認証が実行されることに留意されたい。第１の認証はホーム・ネットワークの中の登録サーバに対してエンド・システムのアイデンティティを認証し、そしてフォーリン・ネットワークとホーム・ネットワークとの相互のアイデンティティを認証する。この機能を実行するために、フォーリン・エージェントは、たとえば、Ｒａｄｉｕｓのアクセス要求パケットの中で、そのローカルＭＳＣの中の登録サーバに対してＩＥＴＦのＲａｄｉｕｓのプロトコルを使ってエンド・システムの登録要求を転送する。エンド・システムのドメイン名を使って、フォーリン登録サーバはそのエンド・システムのホーム・ネットワークおよびホーム登録サーバのアイデンティティを知り、そしてＲａｄｉｕｓのプロキシとして動作し、その要求をそのエンド・システムのホーム登録サーバに対してカプセル化して転送する。フォーリン登録サーバがそのエンド・システムのホームのアイデンティティを知ることができなかった場合、それはオプションとしてＲａｄｉｕｓの要求を、１つのブローカ（たとえば、無線サービス・プロバイダのコンソーシアムによって所有されているもの）のように働く登録サーバに対して転送し、その登録サーバは順にそのＲａｄｉｕｓのアクセス要求を最終のホーム登録サーバに対して代行することができる。ローカルの登録サーバがその登録要求にローカルにあるいは代行によってサービスすることができない場合、それはそのフォーリン・エージェントの登録要求をリジェクトし、そのフォーリン・エージェントはエンド・システムの登録要求をリジェクトする。Ｒａｄｉｕｓのアクセス要求を受信すると、ホーム登録サーバはそのフォーリン・ネットワークおよびエンド・システムのアイデンティティの必要な認証を実行する。認証および登録が成功した場合、そのホーム登録サーバはフォーリン登録サーバに対してＲａｄｉｕｓのアクセス応答パケットで応答し、そのフォーリン登録サーバは応答をフォーリン・エージェントに対して送り、回遊を完了させることができる。ホーム登録サーバが何らかの理由のために適合できない場合、その登録要求はリジェクトされる。

【００９３】第２レベルの認証はイントラネットまたはＩＳＰ ＰＰＰサーバに対するエンド・システムのアイデンティティを検証する。ＰＰＰの認証はモビリティの認証とは別に、インフラストラクチャの装置がＩＳＰから別に配備され、そして所有されることを可能にする。

【００９４】図１４はローミング中のエンド・システムに対する登録のシーケンスを示しているラダー・ダイアグラムである。ＰＰＰサーバおよびホームＩＷＦは同じ

サーバの中にあって、Ｌ２ＴＰは不要であると仮定されている。アカウンティング・サーバが登録中のエンド・システムの代わりにアカウンティングを開始させることおよび、ディレクトリ・サーバがホーム登録サーバのアイデンティティを知ることおよび、エンド・システムのアイデンティティを認証することによる対話に留意されたい。アカウンティング、料金請求、ローミング（サービス・プロバイダ間での）および清算に関する詳細は以下に提供される。

【００９５】エンド・システムのユーザ登録エージェントからのＭＡＣ層メッセージを使ってエージェントの要請を起動することができる。簡単のために、ＭＡＣ層のメッセージは示されない。

【００９６】図１４において、エンド・システム（モバイル）は最初に報告を要請し、そしてフォーリン・エージェントはそのフォーリン・エージェントのケア・オブ・アドレスを含んでいるそのフォーリン・エージェントが所属するネットワークに関する情報をエンド・システムに提供する公示によって応答する。代わりに、このフェーズを取り除くことができ、そしてすべてのネットワーク公示が絶えず発信されているＭＡＣ層のビーコン・メッセージによって行われるようにすることができる。この場合、そのネットワークはフォーリン無線サービス・プロバイダであると仮定される。次に、（エンド・システムの中の）ユーザ登録エージェントはフォーリン・エージェントに関する情報（ユーザ名および他のセキュリティの信用証明を含んでいる）およびそのネットワークに関する情報を１つの要求の中に組み込み、その要求をフォーリン・エージェントに対して送信する。そのフォーリン・エージェントはプロキシ登録エージェントとして、フォーリン登録サーバ（すなわち、そのフォーリン無線サービス・プロバイダに対する登録サーバ）に対してその要求を中継する。次に、そのフォーリン登録サーバは、それがホーム・ディレクトリにないことを認識して、フォーリン無線サービス・プロバイダの中のＦＤＤによってフォーリン・ディレクトリ・サーバにアクセスし、その登録要求をエンド・システムが所属している無線サービス・プロバイダのホーム登録サーバに対してどのように振り向けるかを知る。そのフォーリン登録サーバは必要な転送情報によって応答する。次にそのフォーリン登録サーバはそのエンド・システムの登録要求をＲａｄｉｕｓのアクセス要求の中にカプセル化し、そのカプセル化された要求を、そのエンド・システムが所属している無線サービス・プロバイダのホーム登録サーバに対して中継する。ホーム登録サーバはそのホーム登録サーバのＨＤＤによってホーム・ディレクトリ・サーバにアクセスし、そのフォーリン・サービス・プロバイダに関して少なくとも認証情報を知る。オプションとして、ホーム登録サーバは加入者のディレクトリにアクセスして詳細の加入者サービス・プロフィール情報（たとえば、加入しているサービスの品質のオプションなど）を知る。すべてのパーティが認証されると、ホーム登録サーバはＩＷＦ開始要求をホームＩＷＦおよびＰＰＰサーバに対して送信する。ホームＩＷＦおよびＰＰＰサーバはホーム・アカウンティング・サーバをスタートさせ、ＩＷＦ開始応答をホーム登録サーバへ送信する。次に、ホーム登録サーバはＲａｄｉｕｓのアクセス応答をフォーリン登録サーバへ送信する。次に、フォーリン登録サーバはサービスしているＩＷＦサーバに対してＩＷＦ開始要求を送信する。サービスしているＩＷＦサーバはサービスしているアカウンティング・サーバをスタートさせてから、ＩＷＦ開始応答をフォーリン登録サーバへ送信する。フォーリン登録サーバは登録応答をフォーリン・エージェントに対して送信し、そしてフォーリン・エージェントはその登録応答をエンド・システムに対して中継する。

【００９７】リンク制御プロトコル（ＬＣＰ）構成要求が、エンド・システムによってフォーリン登録サーバを通じてホームＩＷＦおよびＰＰＰサーバに対して送信される。ホームＩＷＦおよびＰＰＰサーバはフォーリン登録サーバを通じてＬＣＰ構成アクノレッジメントをエンド・システムに対して送信する。

【００９８】同様に、パスワード認証プロトコル（ＰＡＰ）認証要求がホームＩＷＦおよびＰＰＰサーバによって送信され、アクノレッジされる。代わりに、チャレンジ認証プロトコル（ＣＨＡＰ）を使って認証することもできる。認証するためにこの両方のプロトコルを使うことができる。あるいはこのフェーズをスキップしてもよい。

【００９９】同様に、ＩＰ構成プロトコル（ＩＰＣＰ）構成要求がホームＩＷＦおよびＰＰＰサーバに対して送信され、それらによってアクノレッジされる。

【０１００】エンド・システムに対するコネクションは次のどれかの理由のためにターミネートされる可能性がある。

１．ユーザ起動ターミネーション。このシナリオにおいては、エンド・システムはまず最初にＰＰＰを順序正しくターミネートする。これはＰＰＰネットワーク制御プロトコル（ＩＰＣＰ）のターミネーションおよびそれに続くＰＰＰリンク・プロトコルのターミネーションを含む。これが行われると、エンド・システムはネットワークから登録解除し、その後、アクセス・ポイントに対する無線リンクのターミネーションを行う。

【０１０１】２．無線リンクの消失。このシナリオはモデムによって検出され、エンド・システムの中のモデム・ドライバに対して報告される。このソフトウェアの上層にはスタックをターミネートしてユーザに通知するよう通知される。

【０１０２】３．フォーリン・エージェントに対するコネクションの消失。このシナリオはエンド・システムの

中のモビリティ・ドライバによって検出される。フォーリン・エージェント（新しいものとなる可能性がある）との連絡を再確立しようとして失敗した後、そのドライバはプロトコル・スタック上に適切な通知を送信し、そして無線リンクをターミネートするための信号も下位のモデムのハードウェアに信号を送る。

【０１０３】４．ＩＷＦに対するコネクションの消失。これはフォーリン・エージェントに対するコネクションの消失の場合と実質的に同じである。

【０１０４】５．ＩＷＦまたはＰＰＰサーバによるＰＰＰのターミネーション。このシナリオはエンド・システムの中のＰＰＰサーバによって検出される。エンド・システムのＰＰＰドライバにはこのイベントが通知される。それはネットワークからの登録解除を開始し、その次にアクセス・ポイントに対する無線リンクのターミネーションが続く。

【０１０５】エンド・システムのサービス・コンフィギュレーションは、その加入者のサービス・プロフィールに基づいてエンド・システムに対してネットワーク・サービスを構成するという概念を指す。加入者のサービス・プロフィールは加入者ディレクトリに格納されている。サービス・プロフィールはソフトウェアがその加入者に代わって無線データ・サービスをカスタマイズすることができるための情報を含んでいる。これはエンド・システムを認証するための情報を含み、それによってそのエンド・システムがロームし、そのエンド・システムのインターネット・サービス・プロバイダに対するコネクションをセットアップすることができる。また、この情報は他のパラメータ、たとえば、サービスの品質などを含むことが好ましい。加入者ディレクトリの他に、ホーム・ドメイン・ディレクトリ（ＨＤＤ）およびフォーリン・ドメイン・ディレクトリ（ＦＤＤ）がローミングのためおよび、フォーリンおよびホームの登録サーバを互いに認証するために使われる。ＨＤＤはエンド・システムのホーム・ネットワークに関する情報を格納し、ＦＤＤは加入者が訪問する可能性のあるフォーリン・ネットワークに関する情報を格納する。

【０１０６】図１５はこれらのディレクトリがネットワーク・アーキテクチャにどのようにマップし、そしてホームにおいて登録しているエンド・システムのための登録の間にどのように使われるかを示している。ステップ０において、エンド・システム（モバイル）はフォーリン・エージェントが所属しているネットワークに関する情報をエンド・システムに提供するフォーリン・エージェントからの公示を要請して受信する。この場合、そのネットワークはホームの無線サービス・プロバイダである。ステップ１において、（エンド・システムの中の）ユーザ登録エージェントが、そのフォーリン・エージェントおよびそれのネットワークおよびそれのセキュリティの信用証明に関する情報を要求の中に組み込み、その

要求をフォーリン・エージェントに対して送信する。ステップ２において、そのフォーリン・エージェントは、プロキシ登録エージェントとして、その要求をホーム登録サーバに対して中継する。ステップ３において、ホーム登録サーバはホーム無線サービス・プロバイダのＨＤＤにアクセスして少なくとも認証情報について知る。ステップ４において、ホーム登録サーバは加入者ディレクトリにアクセスして詳細の加入者サービス・プロフィール情報（たとえば、加入されているサービスの品質のオプションなど）を知る。ステップ５において、ホーム登録サーバはそのアクセス応答についてフォーリン・エージェントに通知する。ステップ６および７において、フォーリン・エージェントは登録応答についてエンド・システム（すなわち、モバイル）に通知する。

【０１０７】図１６はフォーリン・ネットワークから登録を行っているエンド・システムに対するディレクトリの使用法を示している。ステップ０において、エンド・システム（モバイル）は公示を要請して受信し、そしてフォーリン・エージェントは、そのフォーリン・エージェントが所属しているネットワークに関する情報をエンド・システムに提供する公示を発生する。この場合、そのネットワークはフォーリンの無線サービス・プロバイダである。ステップ１において、（エンド・システムの中の）ユーザ登録エージェントがそのフォーリン・エージェントおよびそれのネットワークおよびそれのセキュリティ信用証明を要求に組み込み、その要求をフォーリン・エージェントに対して送信する。ステップ２において、そのフォーリン・エージェントは、プロキシ登録エージェントとして、その要求をフォーリン登録サーバ（すなわち、そのフォーリン無線サービス・プロバイダに対する登録サーバ）に対して中継する。ステップ３において、フォーリン登録サーバはフォーリン無線サービス・プロバイダのＨＤＤにアクセスし、エンド・システムが所属しているネットワークについて知る。ステップ４において、フォーリン登録サーバはエンド・システムの要求をそのエンド・システムのホーム無線サービス・プロバイダのホーム登録サーバに対して転送する。ステップ５において、ホーム登録サーバはホーム登録サーバのＦＤＤにアクセスして、少なくともそのフォーリン・サービス・プロバイダに関する認証情報を知る。ステップ６において、ホーム登録サーバはその加入者のディレクトリにアクセスして詳細の加入者サービス・プロフィール情報（たとえば、加入されているサービスの品質のオプションなど）を知る。ステップ７において、ホーム登録サーバはそのアクセス応答についてフォーリン登録サーバに通知する。ステップ８において、フォーリン登録サーバはそのアクセス応答をフォーリン・エージェントに対して転送する。ステップ９において、フォーリン・エージェントはその登録応答についてエンド・システム（すなわち、モバイル）に通知する。

【０１０８】プロトコル処理のシナリオは、ベアラ・データおよび、ベアラ・データをエンド・システムとの間で搬送するための関連付けられたスタックを処理する。セル・アーキテクチャに対するプロトコル・スタックはローカルのＡＰ（図１７）およびリモートのＡＰ（図１８）を使用する。

【０１０９】図１７は（そのホーム・ネットワークの中の）エンド・システムとホームにあるエンド・システムに対するホームＩＷＦとの間の通信を処理するためのプロトコル・スタックを示している。図１７はアクセス・ポイントおよび無線ハブが同じ場所にある場合のセル・アーキテクチャに対するプロトコル処理を示している。

【０１１０】図１８はアクセス・ポイントが無線ハブから離れた場所にある場合のセル・アーキテクチャに対するプロトコル処理を示している。図に示されているように、ＰＰＰはＩＷＦにおいてターミネートし、その構成は直接のインターネット・アクセスを提供する。ＰＰＰサーバがＩＷＦから別れている場合の構成が後で説明される。

【０１１１】図１８において、エンド・システムからのＰＰＰフレームはＲＬＰ（無線リンク・プロトコル）フレームの中にカプセル化され、そのＲＬＰフレームは幹線アクセス・ポイント（すなわち、その無線ハブの近くに物理的に置かれているアクセス・ポイント）と通信するためのＭＡＣフレームの中にリモートのアクセス・ポイントにおいてカプセル化され、そのリモートのアクセス・ポイントはそのアクセス・ポイントに対して、たとえば、無線幹線によって結合されている。アクセス・ポイントはＭＡＣ層のブリッジとして機能し、エア・リンクからのフレームを無線ハブの中のフォーリン・エージェントに対して中継する。フォーリンエージェントはＭＡＣフレームからＲＬＰフレームをカプセルから取り出し、ｘｔｕｎｎｅｌプロトコルを使って、そのＲＬＰフレームをＩＷＦに対して中継する。同様に、逆の場合にも、フレームをＩＷＦからエンド・システムに対して送信するためのプロセスが発生する。

【０１１２】エンド・システムが別のフォーリン・エージェントへ移動する場合、その新しいフォーリン・エージェントとＩＷＦとの間に新しいｘｔｕｎｎｅｌが自動的に生成され、ＰＰＰトラヒックが中断されずにそれらの間で流れ続けるようにする。

【０１１３】リモートのＡＰと幹線ＡＰとの間に無線幹線を使っているリモートのＡＰセル・アーキテクチャ（図１８）において、エンド・システムとアクセス・ポイントとの間のエア・リンクはその幹線の周波数（ｆ２）とは異なる周波数（ｆ１）で動作し、異なる無線技術を使うことができる。

【０１１４】図１９はロームしているエンド・システムに対するプロトコル・スタックを示している。サービスしているＩＷＦはそのサービスしているＩＷＦとホームＩＷＦとの間でＩ－ｘｔｕｎｎｅｌプロトコルを使用する。プロトコル・スタックの残りの部分は変らず、図には示されていない。このアーキテクチャはサービスしているＩＷＦを基地局に併合することによって単純化することができ、それによってＸＷＤプロトコルをなくすことができる。

【０１１５】ＲＬＰ層はシーケンス番号を使って、重複しているＰＰＰデータグラムをドロップし、そしてエンド・システムとＩＷＦとの間でＰＰＰデータグラムのイン・シーケンスの配送を提供する。また、それはエンド・システムとＩＷＦとの間のリンクの接続性を監視するための構成設定可能な活性化保持（ｋｅｅｐ－ａｌｉｖｅ）メカニズムを提供する。さらに、他の実施形態においては、ＲＬＰ層はエンド・システムとＩＷＦとの間のリンクの総合的なビット・エラー・レートを減らすために、再送信およびフロー制御のサービスも提供する。エンド・システムとＩＷＦとの間のＲＬＰはそのセッションの先頭において開始され、そしてそのセッション全体を通じて、ハンドオフに際してもアクティブのままになっている。

【０１１６】モバイルのＩＰ　ＲＦＣ（ＲＦＣ　２００３）における仕様とは対照的に、ＩＰのカプセル化におけるＩＰはフォーリン・エージェントとホームＩＷＦとの間のトンネリングのためには使われない。代わりに、ＵＤＰのトップに実装される新しいトンネリング・プロトコルが使われる。このトンネリング・プロトコルはＬ２ＴＰプロトコルの単純化されたバージョンである。この選定の理由は次の通りである。

【０１１７】１．ＲＦＣ　２００３の中で規定されているカプセル化のプロトコルは、パケットのフロー制御またはイン・シーケンスの配送を提供しない。現在説明されているネットワークは、バックホール上のトンネルの中でこれらのサービスを必要とする可能性がある。基地局とＭＳＣとの間のネットワーク上でのフロー制御の問題に起因するパケットの消失のため、あるいは基地局またはＩＷＦにおけるフロー制御の問題のために、エア・リンク上での再送信の量を減らすためにフロー制御が必要となる可能性がある。

【０１１８】２．ＵＤＰベースのトンネリング・プロトコルを使うことによって、それをユーザ・レベルで実装することができ、その後、それがデバッグされてから、性能の理由のためにカーネルの中に入れることができる。

【０１１９】３．ＲＦＣ　２００３を使って、サービスの品質および負荷バランシングを考慮に入れてトンネルを生成する簡単な方法はない。ＱＯＳを考慮に入れるために、必要なＱＯＳをすでに提供しているリンク上でトンネルをセットアップすることができなければならない。第２に、ＲＦＣ　２００３を使って、基地局とＭＳＣとの間の多重リンク上で運送者のトラヒックの負荷を

分散させるための負荷バランシングを提供するための簡単な方法はない。

【０１２０】４．ＲＦＣ　２００３に規定されているようなＩＰのカプセル化においてＩＰを実装するためには、開発者はＩＰのソース・コードにアクセスする必要がある。商用のオペレーティング・システムにおいては、ＴＣＰ／ＩＰスタックに対するソース・コードは一般に他の装置製造者に所有権がある。ベンダーからＴＣＰ／ＩＰスタックを購入し、モバイルのＩＰトンネリングをサポートするためにＩＰ層に対して変更を行うことは、開発者が各種のバージョンのＴＣＰ／ＩＰスタックをサポートし続ける必要があることになる。これはコストおよびリスクが増える。

【０１２１】基地局とＩＷＦとの間のトンネリング・プロトコルは非標準であり、そして無線サービス・プロバイダは異なるベンダーからの装置をミックスしてマッチさせることはできないことに留意する必要があるが、単独の無線サービス・プロバイダ・ネットワーク内での非標準のトンネリング・プロトコルの使用は、エンド・システムおよび他のベンダーからの装置にとってはトランスペアレントである。

【０１２２】新しいトンネリング・プロトコルはＬ２ＴＰに基づいている。それ自身、Ｌ２ＴＰは重量級のトンネリング・プロトコルであり、Ｌ２ＴＰにはトンネルの生成および認証に関連して多くのオーバーヘッドがある。本発明のシステムの新しいトンネリング・プロトコルのオーバーヘッドは少ない。この新しいｘｔｕｎｎｅｌプロトコルは次の特徴を有する。

【０１２３】１．ｘｔｕｎｎｅｌの生成は基地局と登録サーバとの間でのＲａｄｉｕｓのアクセス要求およびＲａｄｉｕｓのアクセス応答のメッセージに対してベンダー固有の拡張を追加する。これらの拡張はトンネルのパラメータをネゴシエートし、そしてトンネルを生成するためのものである。

【０１２４】２．登録サーバは異なるＩＰアドレス、したがって、ＭＳＣの中の異なるサーバに対してパケットをトンネルし、中継する実際の作業を代行することができる。これによって、登録サーバが複数のＩＷＦサーバにわたって負荷バランシングを行うことができ、そして各種のユーザに対して異なるＱＯＳを提供することができる。

【０１２５】３．ｘｔｕｎｎｅｌのプロトコルはイン・バンドの制御メッセージをトンネルの管理のためにサポートする。これらのメッセージはトンネルの接続性をテストするためのエコー要求／応答、トンネルを切り離すための切り離し要求／応答／通知、およびエラーを通知するためのエラー通知を含む。これらのメッセージはトンネリングのメディア、たとえば、ＵＤＰ／ＩＰ上で送信される。

【０１２６】４．ｘｔｕｎｎｅｌのプロトコルはトンネリング・メディア、たとえば、ＵＤＰ／ＩＰ上でペイロード・データを送信する。ｘｔｕｎｎｅｌのプロトコルはフロー制御およびイン・シーケンスのパケットの配送をサポートする。

【０１２７】５．ｘｔｕｎｎｅｌのプロトコルはサービスの品質のためにＵＤＰ／ＩＰ以外のメディア上で実装することができる。

【０１２８】ネットワークはホームＩＷＦにおけるＰＰＰをターミネートし、標準のＩＰルーティング技法を使ってルーター経由でインターネットに対してＩＷＦからＩＰパケットを回送することにより、インターネットの直接の接続性をサポートする。ＩＷＦは情報ルーティング・プロセス（ＲＩＰ）を実行することが好ましく、ルータもＲＩＰおよび、場合によってはオープン・ショーテスト・パス・ファースト（ＯＳＰＦ）などの他の可能なルーティング・プロトコルを実行することが好ましい。

【０１２９】このネットワークはインターネット・サービス・プロバイダでもある無線サービス・プロバイダに対して第１の構成をサポートする。この構成においては、ＭＳＣの中のホームＩＷＦのＰＰＰサーバとして機能する。また、このＩＷＦはＲＩＰなどのインターネット・ルーティング・プロトコルを実行し、そしてルーターを使ってインターネットのサービス・プロバイダのバックボーン・ネットワークに接続する。

【０１３０】このネットワークは、無線サービス・プロバイダ（ＷＳＰ）自身がＩＳＰでないため、あるいはそのＷＳＰがエンド・ユーザに対してアクセスを提供するために他のＩＳＰと契約しているため、の何れかの理由で、エンド・システムが１つまたはそれ以上のインターネット・サービス・プロバイダに接続することを許したい無線サービス・プロバイダに対して、第２の構成をサポートする。たとえば、無線サービス・プロバイダはネットワーク・アクセスをエンド・ユーザに対して提供することを選択することができ、そしてそのＷＳＰネットワークからＩＳＰにアクセスするためのサード・パーティのＩＳＰとのアカウントを有しているユーザを許可するために、サード・パーティのＩＳＰと契約することができる。この構成においては、ＰＰＰサーバはＭＳＣにおいてインストールされているホームＩＷＦの中では実行しない。代わりに、Ｌ２ＴＰ（レイヤ２のトンネリング・プロトコル）などのトンネリング・プロトコルが、そのＩＳＰのＰＰＰサーバに対してトンネル・バックするために使われる。図１０はホームにあるエンド・システムに対するこの構成のためのプロトコル・スタックを示している。

【０１３１】ホームＩＷＦおよびＩＳＰのＰＰＰサーバのロケーションは、そのＰＰＰセッションの間中、固定に保たれている。また、ＩＷＦとそのＩＳＰのＰＰＰサーバとの間のＬ２ＴＰトンネルもそのＰＰＰセッション

の間中、そのままになっている。ＩＷＰとＰＰＰサーバとの間の物理リンクは専用のＴ１またはＴ３またはフレーム・リレーまたはＡＴＭネットワークを使っている１つのルーターを経由している。物理リンクの実際の性質はアーキテクチャーの観点からは重要ではない。

【０１３２】この構成はイントラネット・アクセスもサポートする。イントラネット・アクセスの場合、ＰＰＰサーバは企業のイントラネットの中に駐在し、そしてホームＩＷＦはＬ２ＴＰを使ってそれに対してトンネルする。

【０１３３】固定型のエンド・システムに対して、イントラネットまたはＩＳＰのアクセスのためのプロトコル処理が図２０に示されており、これはロームしているエンド・システムがサービスしているＩＷＦを使ってそのホームＩＷＦに接続するということが異なっている。サービスしているＩＷＦとホームＩＷＦとの間のプロトコル処理については以前に説明されている。図２０においては、ホームＩＷＦは無線ハブに併合され、ＸＴｕｎｎｅｌプロトコルをなくすことができる。また、サービスしているＩＷＦを無線ハブに併合し、それによってＸＴｕｎｎｅｌのプロトコルを無くすことができる。

【０１３４】図２１はローカルのＡＰセルのアーキテクチャのための登録フェーズ（エンド・システムの登録）の間に使われるプロトコル・スタックを示している。リモートのＡＰセル・アーキテクチャに対するスタックは非常によく似ている。

【０１３５】上で示されたシナリオはロームしているエンド・システムに対するシナリオである。ホームにあるエンド・システムの場合、登録経路の中にフォーリン登録サーバはない。

【０１３６】エンド・システムの中のモビリティ・エージェントに留意されたい。エンド・システムの中のモビリティ・エージェントと無線ハブの中のフォーリン・エージェントとは、概念的にはモバイルＩＰ　ＲＦＣ　２００２に類似している。モビリティ・エージェントはタイムアウトおよび再試行を使ってネットワークのエラーを扱う。ベアラ・データのための既知のプロトコル・スタックと違って、ＲＬＰは使われない。フォーリン・エージェントおよび登録サーバはＵＤＰ／ＩＰ上でＲａｄｉｕｓを使って、エンド・システムを登録するために互いに通信する。

【０１３７】セキュリティのいくつかの態様が考慮されなければならない。第１は、無線登録フェーズの間でのエンド・システムおよびフォーリン／ホームのネットワークのアイデンティティを認証することである。第２は、ＰＰＰ認証フェーズの間にＰＰＰサーバによってエンド・システムのアイデンティティを認証することである。第３は、アカウンティング・データを格納するため、料金請求のため、およびホーム・ドメインの情報の更新のための認証である。第４は、エンド・システムとの間で転送されるベアラ・トラヒックの暗号化である。第５は、サービス・プロバイダの境界にまたがる料金請求情報の交換のための暗号化である。

【０１３８】エンド・システムのそれぞれのホーム・ネットワークによるアイデンティティおよびホームおよびフォーリンのネットワークの無線登録時の互いのアイデンティティを認証するために共有の秘密のキーが使われる。

【０１３９】エンド・システムの認証はその登録要求のための認証指示子を生成するために１２８ビットの共有の秘密のキーを使う。その認証指示子は、モバイルＩＰ　ＲＦＣ　２００２の中で記述されているような既知のＭＤ５メッセージ・ダイジェスト・アルゴリズムを使って生成される。代わりに、異なるアルゴリズムを使うことができる。その共有の秘密のキーはエンド・システムによる登録要求の中では送信されない。認証指示子だけが送信される。エンド・システムからの登録要求を受信すると、ホーム登録サーバは共有の秘密のキーを使って登録要求データ上で認証指示子を再計算する。計算された認証指示子の値がエンド・システムから送られてきた認証指示子の値とマッチした場合、ホーム登録サーバは登録プロセスの進行を許可する。その値がマッチしなかった場合、ホーム登録サーバはそのイベントをログし、セキュリティ違反警報およびＮＡＫ（すなわち、指定のアクノレッジメント）をその要求に対して発生する。

【０１４０】登録応答において、ホーム登録サーバは同じことを行う。すなわち、共有の秘密のキーを使って、エンド・システムに対して送信する登録応答のための認証指示子を生成する。その応答を受信すると、エンド・システムは共有の秘密のキーを使ってその認証指示子を再計算する。その値が応答の中でホーム登録サーバから送られてきた認証指示子の値とマッチしなかった場合、エンド・システムはその応答を捨て、再試行する。

【０１４１】これらのネットワーク・セキュリティの概念はモバイルＩＰ　ＲＦＣ　２００２の中で定義されている概念に似ている。ＲＦＣによると、モビリティのセキュリティの関連付けが各エンド・システムとそのホーム・ネットワークとの間に存在する。各モビリティのセキュリティの関連付けはセキュリティ・コンテクストの収集を定義する。各セキュリティ・コンテクストは認証のアルゴリズム、モード、秘密のキー（共有されているか、あるいはパブリック - プライベート）、再生保護のスタイルおよび使用する暗号のタイプを定義する。本発明のネットワークのコンテクストにおいては、エンド・システムのユーザ名（モバイルのＩＰのホーム・アドレスの代わりに）が、エンド・システムとそのホーム・ネットワークとの間のモビリティのセキュリティの関連付けを識別するために使われる。セキュリティ・パラメータ・インデックス（ＳＰＩ）と呼ばれる別のパラメータが、モビリティのセキュリティの関連付けの中でセキュ

リティ・コンテクストを選択するために使われる。本発明の基本的な実施形態においては、デフォルトのモバイルＩＰ認証アルゴリズム（キー付きのＭＤ５）およびデフォルトのモード（「プリフィックス＋サフィックス」）が１２８ビットの共有の秘密のキーによってサポートされる。ネットワーク・ユーザはそれぞれのホーム・ネットワークとの複数の共有型の秘密のキーを定義することが許されている。エンド・システムに対するセキュリティ・コンテクストを生成するため、各セキュリティ・コンテクストに対してＳＰＩを割り当てるため、およびセキュリティ・コンテクストの内容（共有の秘密のキーを含む）を設定するため、およびそれぞれの内容を修正するためのメカニズムが以下に説明される。登録時に、１２８ビットのメッセージ・ダイジェストがＭＤ５のアルゴリズムを使ってプリフィックス＋サフィックスのモードでエンド・システムによって計算される。その共有の秘密のキーはその登録要求の中で保護されるべきデータに対するプリフィックスおよびサフィックスとして使われる。このようにして計算された認証指示子は、ＳＰＩおよびユーザ名と一緒に登録要求の中でエンド・システムによって送信される。エンド・システムの登録要求を受け取ると、フォーリン予約サーバはその認証指示子およびＳＰＩと一緒に、要求を不変のままホーム登録サーバに対して中継する。エンド・システムから直接に、あるいはフォーリン登録サーバ経由で間接にその登録要求を受信すると、ホーム登録サーバはそのＳＰＩおよびユーザ名を使ってそのセキュリティ・コンテクストを選択する。ホーム・サーバは共有の秘密のキーを使ってその認証指示子を再計算する。その計算された認証指示子の値がエンド・システムによってその要求の中で送られてきた認証指示子の値とマッチした場合、そのユーザのアイデンティティは正しく認証されたことになる。そうでなかった場合、ホーム登録サーバはエンド・システムから送られてきた登録要求に対してｎａｋ（否定のアクノレッジメント）を返す。

【０１４２】ホーム登録サーバによってエンド・システムに対して送られてきた登録応答も、上記のアルゴリズムを使って認証される。ＳＰＩおよび計算された認証指示子の値が、登録応答メッセージの中でホーム・サーバによってエンド・システムに対して送信される。その応答を受信すると、エンド・システムはその認証指示子を再計算し、そしてその計算された値が送信されてきた値とマッチしなかった場合、その応答を捨てて再試行する。

【０１４３】ユーザのエンド・システムはそのユーザが自分の登録サーバと共有するすべてのセキュリティ・コンテクストに対して、共有の秘密のキーおよびＳＰＩによって構成されなければならない。このコンフィギュレーション情報は、Ｗｉｎｄｏｗｓ　９５ベースのエンド・システムの場合はＷｉｎ　９５のレジストリに格納することが好ましい。登録時に、この情報がアクセスされ、認証の目的のために使われる。

【０１４４】ネットワークにおいては、エンド・システムを登録するため、および無線ハブとホームおよびサービスしているＩＷＦとの間のｘｔｕｎｎｅｌをエンド・システムに代わって構成するために、Ｒａｄｉｕｓのプロトコルがフォーリン・エージェントＦＡによって使われる。エンド・システムから登録要求を受信すると、そのＦＡはＲａｄｉｕｓのアクセス要求パケットを生成し、それ自身の属性をそのパケットに格納し、エンド・システムの登録要求属性をそのまま変えずにこのパケットにコピーし、その組み合わせられた要求をＭＳＣの中の登録サーバに対して送信する。

【０１４５】Ｒａｄｉｕｓの認証はＲａｄｉｕｓのクライアント（この場合、基地局の中のＦＡ）およびＲａｄｉｕｓのサーバ（この場合、ＭＳＣの中の登録サーバ）が認証の目的のための秘密のキーを共有することを必要とする。この共有の秘密のキーはＲａｄｉｕｓのクライアントとＲａｄｉｕｓのサーバとの間で通信されるすべてのプライベート情報を暗号化するためにも使われる。その共有の秘密のキーは構成設定可能なパラメータである。ネットワークはＲａｄｉｕｓのＲＦＣの中の推奨に従い、共有の秘密のキーおよびＭＤ５のアルゴリズムを、認証のため、および暗号化のために、暗号化が必要とされる場所で使う。ＦＡによって送信されるＲａｄｉｕｓのアクセス要求パケットは、Ｒａｄｉｕｓのユーザ名属性（エンド・システムによって提供される）およびＲａｄｉｕｓのユーザ・パスワード属性を含んでいる。ユーザ・パスワード属性の値も構成設定可能な値であり、Ｒａｄｉｕｓのプロトコルによって推奨される方法で暗号化される。ＲａｄｉｕｓのＲＦＣ標準の観点からは非標準の属性であるネットワーク固有の他の属性は、ベンダー固有のＲａｄｉｕｓの属性として符号化され、アクセス要求パケットの中で送信される。

【０１４６】次の属性がＦＡによってＲａｄｉｕｓのアクセス要求パケットの中でその登録サーバに対して送信される。

１．ユーザ名属性：これはエンド・システムの登録要求の中でエンド・システムによって供給されるエンド・システムのユーザ名である。

【０１４７】２．ユーザ・パスワード属性：このユーザ・パスワードはユーザに代わって基地局／無線ハブによって供給される。それは基地局とその登録サーバとの間で共有の秘密のキーを使って、ＲａｄｉｕｓのＥＦＣにおいて記述されているように符号化される。

【０１４８】３．ＮＡＳポート：これは基地局におけるポートである。

【０１４９】４．ＮＡＳ－ＩＰアドレス：これは基地局のＩＰアドレスである。

【０１５０】５．サービス・タイプ：これはフレーム型

のサービスである。

【０１５１】６．フレーム型のプロトコル：これはＰＰＰプロトコルである。

【０１５２】７．Ｘｔｕｎｎｅｌプロトコル・パラメータ：これらのパラメータはエンド・システムに代わってＸＴｕｎｎｅｌプロトコルをセットアップするのに必要なパラメータを指定するために、基地局によって送信されるパラメータである。

【０１５３】８．ＡＰ－ＩＰアドレス：これはユーザがそれを通して登録しているＡＰのＩＰアドレスである。これはベンダー固有の属性である。

【０１５４】９．ＡＰのMACアドレス。これは１０までのＡＰのMACアドレスである。

【０１５５】１０．エンド・システムの登録要求：エンド・システムからの登録要求が不変のまま、このベンダー固有の属性にコピーされている。

【０１５６】次の属性がＦＡに対してＲａｄｉｕｓのアクセス要求パケットの中で登録サーバから送信される。

１．サービス・タイプ：これはフレーム型のサービスである。

２．フレーム型のプロトコル：これはＰＰＰである。

３．ＸＴｕｎｎｅｌプロトコルのパラメータ：これらのパラメータはエンド・システムに代わってｘｔｕｎｎｅｌのプロトコルをセットアップするために必要なパラメータを指定するために登録サーバによって送信される。これはベンダー固有の属性である。

４．ホーム登録サーバの登録応答：この属性はＦＡに対してホーム登録サーバから送信される。ＦＡはこの属性を不変のまま、エンド・システムに対して登録応答パケットの中で中継する。その経路の中にフォーリン登録サーバがあった場合、この属性はそれによってＦＡによって不変のまま中継される。それはベンダー固有の属性として符号化されている。

【０１５７】エンド・システムのローミングに対するサービスを提供すめに、フォーリンネットワークおよびホーム・ネットワークは認証およびコンフィギュレーションのためのＲａｄｉｕｓのプロトコルを使って、アカウンティングおよび料金請求の目的のために互いに認証される。この認証はエンド・システムの登録の時点で実行される。以前に説明されたように、フォーリン・ネットワークの中の登録サーバがエンド・システムからの登録要求（ＦＡによってＲａｄｉｕｓのアクセス要求パケットの中のベンダー固有の属性としてカプセル化されている）を受け取ると、それはそのエンド・システムのユーザ名を使って、そのホーム・ドメイン・ディレクトリＨＤＤを参照することにより、そのエンド・システムのホーム登録サーバのアイデンティティを知る。次の情報がホーム・ドメイン・ディレクトリＨＤＤの中に格納されており、エンド・システムの登録要求を転送するためにフォーリン登録サーバによってアクセスされる。

【０１５８】１．ホーム登録アドレスのＩＰアドレス：これは登録要求を転送するためのホーム登録サーバのＩＰアドレスである。

【０１５９】２．フォーリン登録サーバ・マシンのＩｄ：これはＳＭＴＰ（単純化されたメイル転送プロトコル）のフォーマット（たとえば、ｍａｃｈｉｎｅ＠ｆｑｄｎここでｍａｃｈｉｎｅはそのフォーリン登録サーバ・マシンの名前であり、ｆｑｄｎはそのフォーリン登録サーバのドメインの完全にクオリファイされたドメイン名である）でのフォーリン登録サーバのマシンＩＤである。

【０１６０】３．トンネリング・プロトコルのパラメータ：これらはサービスしているＩＷＦとホームＩＷＦとの間のトンネルを、エンド・システムに代わって構成するためのパラメータである。これらはそれらの間で使われるべきトンネリング・プロトコルおよびそのトンネルを構成するためのパラメータを含む。

【０１６１】４．共有の秘密のキー：これはフォーリン登録サーバとホーム登録サーバとの間での認証のために使われるべき共有の秘密のキーである。この秘密のキーはフォーリン登録サーバからホーム登録サーバに対して送信されるＲａｄｉｕｓのパケットの中の、Ｒａｄｉｕｓのユーザ・パスワード属性を計算するために使われる。それは２つの無線サービス・プロバイダの間で定義される。

【０１６２】５．ユーザ・パスワード：これはロームしているエンド・システムに代わって使われるユーザ・パスワードである。このユーザ・パスワードは２つの無線サービス・プロバイダで定義される。このパスワードはＲａｄｉｕｓのＲＳＣにおいて説明されたような共有の秘密のキーを使って暗号化される。

【０１６３】６．アカウンティング・パラメータ：これらは登録中のエンド・システムに代わってアカウンティングを構成するためのパラメータである。これらのパラメータは登録サーバによってエンド・システムに代わってアカウンティングを構成するために、そのＩＷＦに対して送信される。

【０１６４】この情報を使って、フォーリン登録サーバはＲａｄｉｕｓのアクセス要求を生成し、それ自身の登録および認証情報をそのＲａｄｉｕｓのアクセス要求に追加し、エンド・システムから送信された登録情報のコピーを不変のままでＲａｄｉｕｓのアクセス要求にコピーし、その組み合わされた要求をホーム登録サーバに対して送信する。

【０１６５】フォーリン登録サーバから（ローミングしているエンド・システムの場合）、あるいはＦＡから直接に（ホームにあるエンド・システムの場合）、Ｒａｄｉｕｓのアクセス要求を受信すると、ホーム登録サーバはそれ自身のディレクトリ・サーバにアクセスしてその共有の秘密のキーを参照し、認証指示子を再計算するこ

とによってローミングのシナリオの中でフォーリン登録サーバのアイデンティティおよびエンド・システムのアイデンティティを検証する。

【０１６６】その要求を正常に処理した後、ホーム登録サーバはＲａｄｉｕｓのアクセス受付け応答パケットを生成し、それを、エンド・システムがローミング中の場合はフォーリン登録サーバに送信し、あるいはそのＲａｄｉｕｓのアクセス要求を受信したＦＡに対して直接に送信する。その応答は登録応答属性を含み、それをＦＡがエンド・システムに対して中継する。

【０１６７】その要求を正しく処理することができなかった場合、ホーム登録サーバはＲａｄｉｕｓのアクセス・リジェクト応答パケットを生成し、それを、そのエンド・システムがローミング中の場合はフォーリン登録サーバに対して送信し、あるいはそのＲａｄｉｕｓのアクセス要求を送って来たＦＡに対して直接に送信する。その応答は登録応答属性を含み、それをＦＡがエンド・システムに対して中継することになる。

【０１６８】ローミングのシナリオにおいては、ホーム登録サーバからの応答がフォーリン登録サーバによって受信される。それはフォーリン登録サーバによって共有の秘密のキーを使って認証される。認証後、フォーリン登録サーバはその応答を処理し、そして順にそれはＲａｄｉｕｓの応答パケット（受付けまたはリジェクト）をＦＡに対して送信する。フォーリン登録サーバはホーム登録サーバのＲａｄｉｕｓの応答パケットからの登録応答属性を不変のまま、Ｒａｄｉｕｓの応答パケットにコピーする。

【０１６９】ＦＡはＲａｄｉｕｓのアクセス応答またはＲａｄｉｕｓのアクセス・リジェクト応答パケットを受信すると、そのＲａｄｉｕｓの応答から登録応答属性を使って登録応答パケットを生成し、その応答をエンド・システムに対して送信し、それによって回遊した登録シーケンスを完了する。

【０１７０】モバイルＩＰ標準はタイム・スタンプを使って、あるいはオプションとして、臨時情報（ｎｏｎｃｅ）を使って登録に対する再生保護が実装されることを規定している。しかし、タイム・スタンプを使う再生保護は、対応しているノード間の十分に同期化された時計を必要とするので、本発明のシステムは、タイム・スタンプを使った再生保護がモバイルＩＰの標準において必須であって、臨時情報を使うことはオプションであっても、臨時情報を使って登録時の再生保護を実施する。しかし、他の実施形態としてタイム・スタンプを使った再生保護も考えられる。

【０１７１】ノード間で使われる再生保護のスタイルは認証のコンテクスト、モード、秘密のキーおよび暗号化のタイプに加えてセキュリティのコンテクストの中に格納されている。

【０１７２】このネットワークはエンド・システムとそ

のＰＰＰサーバとの間でＰＰＰ　ＰＡＰ（パスワードの認証）およびＣＨＡＰ（チャレンジ認証パスワード）の使用をサポートする。これは以前に説明された登録および認証のメカニズムとは独立に行われる。これによって、プライベート・イントラネットまたはＩＳＰがそのユーザのアイデンティティを独立に検証することができる。

【０１７３】アカウンティングおよびディレクトリのサービスに対する認証がアカウンティングのセキュリティに関して以下に説明される。同じＭＳＣの中でのネットワーク装置からのディレクトリ・サーバへのアクセスは認証される必要がない。

【０１７４】このネットワークはエンド・システムとホームＩＷＦとの間で送信されるベアラ・データの暗号化をサポートする。エンド・システムは適切なセキュリティ・コンテクストを選択することによって暗号化をオンまたはオフするようにネゴシエートする。登録要求を受信すると、ホーム登録サーバはそのセキュリティ・コンテクストに基づいて、そのエンド・システムの要求を暗号化することを許可する。認証のアルゴリズム、モード、共有の秘密のキーおよび再生保護のスタイルを格納するのに加えて、セキュリティ・コンテクストも、使用する暗号化のアルゴリズムのスタイルを指定するために使われる。暗号化がエンド・システムとホーム・エージェントとの間でネゴシエートされた場合、ＰＰＰフレーム全体が、ＲＬＰの中にカプセル化される前にそのように暗号化される。

【０１７５】ＩＷＦ、アカウンティング・サーバおよび料金請求システムはＭＳＣの中の同じ信頼されるドメインの一部である。これらのエンティティは所有されている信頼されるイントラネットの同じＬＡＮまたはその一部のいずれかに接続されている。ＩＷＦとアカウンティング・サーバとの間、およびアカウンティング・サーバとその顧客の料金請求システムとの間のアカウンティングの統計情報の転送を、ＩＰ－ＳｅｃなどのインターネットのＩＰセキュリティ・プロトコルを使って暗号化することができる。

【０１７６】このネットワークはエンド・システムのロケーションを監視するのをさらに難しくしている。というのは、エンド・システムとの間で転送されるすべてのＰＰＰフレームは、そのエンド・システムの装置の実際の場所とは無関係にホームＩＷＦを通過するからである。

【０１７７】アカウンティングのデータはネットワーク内のサービスしているＩＷＦおよびホームＩＷＦによって収集される。サービスしているＩＷＦによって収集されるアカウンティング・データは、サービスしているＩＷＦのＭＳＣの中のアカウンティング・サーバに対して送信される。ホームＩＷＦによって収集されたアカウンティング・データはホームＩＷＦのＭＳＣの中のアカウ

ンティング・サーバに対して送信される。サービスしているＩＷＦによって収集されたアカウンティング・データは、無線サービス・プロバイダの境界にまたがる料金請求情報の監査および清算のために、フォーリン無線サービス・プロバイダによって使われる（ローミングおよびモビリティをサポートするために）。ホームＩＷＦによって収集されたアカウンティング・データは、エンド・ユーザに料金を請求するために使われ、そしてまた、ローミングおよびモビリティを扱うために、無線サービス・プロバイダの境界にまたがる清算のためにも使われる。

【０１７８】エンド・システムのロケーションおよびフォーリン・エージェントのロケーションとは無関係に、すべてのデータ・トラヒックはホームＩＷＦを通って流れるので、ホームＩＷＦは顧客に対する請求書を作成するためのすべての情報および、またはフォーリン・ネットワークの使用に対する清算情報を発生するためのすべての情報を有している。

【０１７９】サービスしているＩＷＦおよびホームＩＷＦは登録されているエンド・システムのためのアカウンティング・レコードを送信するために、Ｒａｄｉｕｓのアカウンティング・プロトコルを使うことが好ましい。Ｒａｄｉｕｓのアカウンティング・プロトコルはＩＥＴＦ　ＲＦＣの草案の中でドキュメント化されているプロトコルである。本発明の場合、そのプロトコルはネットワークに対してベンダー固有の属性を追加することによって、そしてＲａｄｉｕｓのアカウンティング・プロトコルに対してチェック・ポインティングを追加することによって拡張されなければならない。このコンテクストにおけるチェック・ポインティングはアカウンティング・レコードが消失する危険性を最小化するために、アカウンティング・データを定期的に更新することを指す。

【０１８０】Ｒａｄｉｕｓのアカウンティング・プロトコルはＵＤＰ／ＩＰ上で実行し、そしてアクノレッジメントおよびタイム・アウトに基づいた再試行を使用する。Ｒａｄｉｕｓのアカウンティング・クライアント（サービスしているＩＷＦまたはホームＩＷＦ）はＵＤＰのアカウンティング要求パケットをそれぞれのアカウンティング・サーバに対して送信し、アカウンティング・サーバはアカウンティング・クライアントに対してアクノレッジメントを送り返す。

【０１８１】ネットワークの中で、アカウンティング・クライアント（サービスしているＩＷＦおよびホームＩＷＦ）はユーザのセッションの開始点においてアカウンティング開始の指示を出し、そしてそのユーザのセッションの終りにおいてアカウンティング停止の指示を出す。そのセッションの途中において、アカウンティング・クライアントはアカウンティングのチェックポイントの指示を出す。対照的に、ＲａｄｉｕｓのアカウンティングＲＦＣはアカウンティング・チェックポイントの指

示を指定しない。本発明のシステムのソフトウェアはこの目的のためにベンダー固有のアカウンティング属性を生成する。このアカウンティング属性はＡｃｃｔ－Ｓｔａｔｕｓ－Ｔｙｐｅ　ｏｆ　Ｓｔａｒｔ（アカウンティング開始の指示）を含んでいるすべてのＲａｄｉｕｓのアカウンティング要求パケットの中に存在する。この属性の値は、そのアカウンティング・レコードがチェック・ポインティングのレコードであるかどうかをアカウンティング・サーバに対して伝えるために使われる。チェック・ポインティングのアカウンティング・レコードは時間の属性を含み、そしてそのセッションの開始からの累積しているアカウンティング・データを含む。本発明においては、チェック・ポイント・パケットを送信する頻度を構成設定することができる。

【０１８２】サービスしているＩＷＦおよびホームＩＷＦは登録フェーズの間にそれぞれのアカウンティング・サーバに対して接続するために、それぞれの登録サーバによって構成される。その構成設定可能なアカウンティング・パラメータとしては、アカウンティング・サーバのＩＰアドレスおよびＵＤＰポート、チェック・ポインティングの頻度、セッション／マルチセッションのＩＤ、およびアカウンティング・クライアントとアカウンティング・サーバとの間で使われる共有の秘密のキーなどがある。

【０１８３】ネットワークは登録されている各エンド・システムに対して次のアカウンティング属性を記録する。これらのアカウンティング属性は、そのセッションの開始時、そのセッションの終了時、およびその途中（チェック・ポイント）においてアカウンティング・クライアントによってそれぞれのアカウンティング・サーバに対して、Ｒａｄｉｕｓのアカウンティング・パケットの中でレポートされる。

【０１８４】１．ユーザ名：これは上記のＲａｄｉｕｓのユーザ名属性と似ている。この属性はユーザを識別するために使われ、すべてのアカウンティング・レコードの中に存在している。そのフォーマットは「ｕｓｅｒ@ｄｏｍａｉｎ」であり、ここでｄｏｍａｉｎはそのユーザのホームの完全にクオリファイされたドメイン名である。

【０１８５】２．ＮＡＳ　ＩＰアドレス：これは上記のＲａｄｉｕｓのＮＡＳ－ＩＰアドレスに似ている。この属性はホームＩＷＦまたはサービスしているＩＷＦを実行しているマシンのＩＰアドレスを識別するために使われる。

【０１８６】３．無線ポート：この属性はユーザに対してサービスを提供しているアクセス・ポイントにおける無線ポートを識別する。この属性はベンダー固有の属性として符号化されている。

【０１８７】４．アクセス・ポイントのＩＰアドレス：この属性はユーザに対してサービスを提供しているアク

セス・ポイントのＩＰアドレスを識別する。この属性はベンダー固有の属性として符号化されている。

【０１８８】５．サービス・タイプ：これは上記のＲａｄｉｕｓのサービス・タイプ属性と似ている。この属性の値はフレーム化されている。

【０１８９】６．フレーム型のプロトコル：これは上記のＲａｄｉｕｓのフレーム型のプロトコル属性と似ている。この属性の値はＰＰＰを示すために設定される。

【０１９０】７．アカウンティング・ステータス・タイプ：これは上記のＲａｄｉｕｓのＡｃｃｔ－Ｓｔａｔｕｓ－Ｔｙｐｅ属性と似ている。この属性の値はＲａｄｉｕｓのクライアントとのユーザのセッションを開始をマークするためのＳｔａｒｔ、およびＲａｄｉｕｓのクライアントとのそのユーザのセッションの終了をマークするためのＳｔｏｐとすることができる。アカウンティング・クライアントの場合、Ａｃｃｔ－Ｓｔａｔｕｓ－Ｔｙｐｅ／Ｓｔａｒｔ属性はエンド・システムの登録時に発生される。Ａｃｃｔ－Ｓｔａｔｕｓ－Ｔｙｐｅ／Ｓｔｏｐ属性は、何らかの理由でエンド・システムが登録を解除するときに発生される。チェックポイントの場合、この属性の値はＳｔａｒｔであり、そのアカウンティング・チェックポイントの属性も存在している。

【０１９１】８．アカウンティング・セッションのＩｄ：これは上記のＲａｄｉｕｓのアカウンティング・セッションＩｄに似ている。ローミングのシナリオにおいては、このセッションＩｄはエンド・システムが登録要求を発行したときにフォーリン登録サーバによって割り当てられる。それは登録シーケンスの間にフォーリン登録サーバに対してホーム登録サーバによって通信される。ホーム・ネットワークおよびフォーリン・ネットワークは両方ともそのＡｃｃｔ－Ｓｅｓｓｉｏｎ－Ｉｄ属性を知っており、アカウンティング・レコードをそれぞれのアカウンティング・サーバに対して送信する間に、この属性を発行することができる。「エンド・システムがホームにある」のシナリオにおいては、この属性はホーム登録サーバによって発生される。登録サーバは、すべてのアカウンティング・レコードの中でそれを発行するＩＷＦに対して、この属性の値を通信する。

【０１９２】９．アカウンティング・マルチセッションＩｄ：これは上記のＲａｄｉｕｓのＡｃｃｔ－Ｍｕｌｔｉ－Ｓｅｓｓｉｏｎ－Ｉｄと似ている。このＩｄはホーム登録サーバによって、登録要求がエンド・システムに代わってＦＡから直接受信されたとき、あるいはフォーリン登録サーバ経由で受信されたときにホーム登録サーバによって割り当てられる。それはフォーリン登録サーバに対して、ホーム登録サーバによってその登録応答メッセージの中で通信される。その登録サーバはこの属性の値をＩＷＦに対して通信し、ＩＷＦはすべてのアカウンティング・レコードの中にそれを入れて送信する。

【０１９３】そのアーキテクチャに対して追加される真

のモビリティによって、エンド・システムが１つのＩＷＦから別のＩＷＦへ移動する場合に、その同じエンド・システムに対する異なるＩＷＦからのアカウンティング・レコードを一緒に関連付けるために、そのＩｄが使われる。ＩＷＦの境界にまたがるハンドオフの場合、Ａｃｃｔ－Ｓｅｓｓｉｏｎ－Ｉｄは異なるＩＷＦから出てくるアカウンティング・レコードに対して異なっている。しかし、Ａｃｃｔ－Ｍｕｌｔｉ－Ｓｅｓｓｉｏｎ－Ｉｄ属性はそのユーザに対してサービスを提供したすべてのＩＷＦによって発行されたアカウンティング・レコードに対して同じである。セッションＩｄおよびマルチＩｄはフォーリン・ネットワークおよびホーム・ネットワークの両方に対して知られているので、それらはこれらの属性をそれぞれのアカウンティング・サーバに対するアカウンティング・レポートの中に入れて発行することができる。このセッションＩｄおよびマルチセッションＩｄによって、料金請求システムは同じ無線サービス・プロバイダにおけるＩＷＦの境界にまたがるアカウンティング・レコードおよび、無線サービス・プロバイダの境界にまたがるアカウンティング・レコードさえも相関付けることができる。

【０１９４】１．アカウンティングの遅延時間：Ｒａｄｉｕｓのアカウンティング遅延時間属性参照。

【０１９５】２．アカウンティング入力オクテット数：Ｒａｄｉｕｓのアカウンティング入力オクテット数参照。この属性はエンド・システムによって送信されるオクテットの数（エンド・システムからそのネットワークへの入力）を追跡管理するために使われる。エア・リンクのオーバヘッド、あるいはＲＬＰによって課せられるオーバヘッドなどはどれもカウントされない。

【０１９６】３．アカウンティング出力のオクテット数：Ｒａｄｉｕｓのアカウンティング出力オクテット数参照。この属性はエンド・システムに対して送られるオクテット（ネットワークからエンド・システムへの出力）の数を追跡管理するために使われる。このカウントはＰＰＰフレームだけを追跡するために使われる。エア・リンクのオーバヘッド、あるいはＲＬＰによって課されるオーバヘッドなどはどれもカウントされない。

【０１９７】４．アカウンティングの認証：Ｒａｄｉｕｓのアカウンティング認証属性参照。この属性の値はサービスしているＩＷＦまたはホームＩＷＦのいずれがそのアカウンティング・レコードを発生するかによって、ローカル（Ｌｏｃａｌ）またはリモート（Ｒｅｍｏｔｅ）となる。

【０１９８】５．アカウンティング・セッションの時間：Ｒａｄｉｕｓのアカウンティング・セッション時間参照。この属性はユーザがサービスを受けていた時間の量を示す。サービスしているＩＷＦによって送信された場合、この属性はユーザがそのサービスしているＩＷＦからサービスを受けていた時間の量を追跡する。ホーム

ＩＷＦによって送信された場合、この属性はそのユーザがそのホームＩＷＦからサービスを受けていた時間の量を追跡する。

【０１９９】６．アカウンティング入力パケット数：Ｒａｄｉｕｓのアカウンティング入力パケット数属性参照。この属性はエンド・システムから受信されたパケットの数を示す。サービスしているＩＷＦの場合、この属性はエンド・システムからサービスしているＩＷＦへ入力されたＰＰＰフレームの個数を追跡する。ホームＩＷＦの場合、この属性はエンド・システムからホームＩＷＦへ入力されたＰＰＰフレームの数を追跡する。

【０２００】７．アカウンティング出力パケット数：Ｒａｄｉｕｓのアカウンティング出力パケット数属性参照。この属性はエンド・システムに対して送信されたパケットの数を示す。サービスしているＩＷＦの場合、この属性はサービスしているＩＷＦによってエンド・システムに対して出力されたＰＰＰフレームの数を追跡する。ホームＩＷＦの場合、この属性はそのホームＩＷＦからエンド・システムに対して送信されたＰＰＰフレームの数を表す。

【０２０１】８．アカウンティング・ターミネートの理由：Ｒａｄｉｕｓのアカウンティング・ターミネートの理由属性参照。この属性はユーザのセッションがターミネートされた理由を示す。さらに、追加の詳細情報を提供するために固有の理由コードも存在する。この属性はそのセッションの終りにおけるアカウンティング・レポートの中にだけ入っている。

【０２０２】９．ネットワークのアカウンティングのターミネートの理由：この属性はセッションをターミネートした詳細理由を示す。この特定の属性はベンダー固有の属性として符号化され、セッションの終りにおけるＲａｄｉｕｓのアカウンティング属性の中でのみレポートされる。標準のＲａｄｉｕｓの属性Ａｃｃｔ‐Ｔｅｒｍｉｎａｔｅ‐Ｃａｕｓｅも存在する。この属性はＡｃｃｔ‐Ｔｅｒｍｉｎａｔｅ‐Ｃａｕｓｅ属性によってカバーされない特定の理由コードを提供する。

【０２０３】１０．ネットワークのエア・リンクのアクセス・プロトコル：この属性はエンド・システムによって使われるエア・リンクのアクセス・プロトコルを示す。この属性はベンダー固有の属性として符号化されている。

【０２０４】１１．ネットワークのバックホール・アクセス・プロトコル：この属性はアクセス・ポイントによってエンド・システムとの間でデータを受け渡すために使われるバックホール・アクセスのプロトコルを示す。この属性はベンダー固有の属性として符号化されている。

【０２０５】１２．ネットワーク・エージェントのマシン名：この属性はホームＩＷＦまたはサービスしているＩＷＦを実行しているマシンの完全にクオリファイされたドメイン名である。この特定の属性はベンダー固有のフォーマットで符号化されている。

【０２０６】１３．ネットワークのアカウンティング・チェック・ポイント：Ｒａｄｉｕｓのアカウンティング ＲＦＣはチェックポイント・パケットを定義しないので、本発明のネットワークの具体例では、この属性を付けたＲａｄｉｕｓのアカウンティング開始パケットを使ってチェックポイントをマークする。チェックポイント属性が不在であることは通常のアカウンティング開始パケットであることを意味する。この属性が存在しているアカウンティング開始パケットは、アカウンティング・チェックポイント・パケットを意味する。アカウンティング停止パケットにはこの属性はない。

【０２０７】この好適な実施形態においては、すべてのアカウンティング・パケットおよびそれに対応している応答は、ＭＤ５および共有の秘密のキーを使って認証されなければならない。そのＩＷＦはそれぞれのＲａｄｉｕｓのアカウンティング・サーバとの通信中に認証のためにそれらによって使われる共有の秘密のキーによって構成される。アカウンティング・サーバと通信するためにＩＷＦによって使われる共有の秘密のキーは、ＭＳＣの中にあるホーム／フォーリンのドメイン・ディレクトリに格納されている。アカウンティングのセキュリティのための共有の秘密のキーは、エンド・システムの登録シーケンスの間にそれぞれの登録サーバによってＩＷＦに対して通信される。

【０２０８】アカウンティング・サーバのソフトウェアはＭＳＣにあるコンピュータの中で実行される。システムの中のアカウンティング・サーバの役割は、ネットワーク要素（ホームおよびサービスしているＩＷＦ）からの生のアカウンティング・データを収集し、そのデータを処理し、そしてそれを無線サービス・プロバイダの料金請求システムに対して転送するために格納することである。アカウンティング・サーバは料金請求システムを含んではいない。代わりに、それは自動または手動のアカウンティング・データ転送メカニズムをサポートする。その自動アカウンティング・データ転送メカニズムを使って、アカウンティング・サーバはＡＭＡのビリング・フォーマットでのアカウンティング・レコードを、顧客の料金請求システムに対してＴＣＰ／ＩＰトランスポート上で転送する。この目的のために、システムはパケット・データのためのＡＭＡのビリング・レコード・フォーマットを定義する。手動転送メカニズムを使って、顧客はそれぞれの料金請求システムに対してアカウンティング・レコードを転送するためのテープを作ることができる。それぞれの仕様に対するテープを作るために、顧客にはアカウンティング・レコードにアクセスするための情報が提供され、顧客がテープに書き込む前にそれらを処理することができるようになっている。

【０２０９】図２２において、ホームまたはサービスし

ているＩＷＦからアカウンティング・サーバによって受信された生のアカウンティング・データが、アカウンティング・サーバによって処理され、格納される。アカウンティング・サーバによって行われる処理は、フィルタリング、ＩＷＦから受信された生のアカウンティング・データの圧縮および相関付けを含む。デュアルのアクティブ／スタンバイ・プロセッサを使っている、可用性の高いファイル・サーバおよびホット・スワップ可能なＲＡＩＤディスクが、データがアカウンティング・サーバを通して搬送されている間に、そのアカウンティング・データをバッファするために使われる。

【０２１０】アカウンティング・サーバはエンド・システムがそのセッションを終了するまで、生のアカウンティング・データの処理を遅らせる。エンド・システムがそのセッションをターミネートすると、アカウンティング・サーバはそのセッションのために収集した生のアカウンティング・データを処理し、アカウンティングの集計レコードをＳＱＬデータベースに格納する。ＳＱＬデータベースに格納されたアカウンティング集計レコードは、１つのＡＳＮ．１符号化ファイルをポイントする。このファイルはそのエンド・システムのセッションに関する詳細のアカウンティング情報を含む。次に、アカウンティング・サーバに格納されていたデータは、料金請求データ転送エージェントによって顧客の料金請求システムに対して転送される。代わりに、無線サービス・プロバイダがそのＳＱＬデータベースおよび／またはＡＳＮ．１符号化ファイルからのアカウンティング・データを、テープ経由で料金請求システムに対して転送することができる。データベースの方式およびＡＳＮ．１符号化ファイルのフォーマットはドキュメント化され、この目的のために顧客が利用できるようになっている。アカウンティング・システムに格納されている処理済みのアカウンティング・データのボリュームが高い方の限界値を超えた場合、アカウンティング・サーバはＮＭＳアラームを発生する。このアラームはアカウンティング・サーバに格納されているデータのボリュームが低い方の限界値以下に下がったときにクリアされる。そのアラームを発生およびクリアするための高い方の限界値および低い方の限界値は構成設定可能である。また、アカウンティング・サーバは格納されているアカウンティング・データの格納期間が構成設定可能なしきい値を超えた場合に、ＮＭＳアラームを発生する。逆に、そのアカウンティング・データの格納期間がしきい値以下に下がると、そのアラームはクリアされる。

【０２１１】加入者ディレクトリは加入者に関する情報を格納するために使われ、ホーム・ネットワークに置かれている。ホーム登録サーバはエンド・システムを認証して登録するために、その登録フェーズの間にこのディレクトリを参照する。各加入者ごとに、加入ディレクトリは次の情報を格納する。

【０２１２】１．ユーザ名：加入者レコードの中のこのフィールドはＳＭＴＰのフォーマット（たとえば、ｕｓｅｒ＠ｆｑｄｎ）になる。ここでｕｓｅｒのサブフィールドはその加入者をその加入者の無線ホーム・ドメインの中で識別し、そしてｆｑｄｎのサブフィールドはその加入者の無線ホーム・ドメインを識別する。このフィールドはエンド・システムによってその登録要求の中で登録フェーズの間に送信される。このフィールドはネットワーク・サービスへの加入時に、その加入者に対して無線サービス・プロバイダによって割り当てられる。このフィールドはＰＰＰにおいて使われているユーザ名のフィールドとは異なっている。

【０２１３】２．モビリティのセキュリティの関連付け：加入者レコードの中のこのフィールドは、加入者とその加入者のホーム・ネットワークとの間にモビリティのセキュリティとの関連付けを含む。上記のように、モビリティのセキュリティの関連付けは各加入者とそのホーム登録サーバとの間に存在する。モビリティのセキュリティの関連付けはセキュリティ・コンテクストの収集を定義する。各セキュリティ・コンテクストは認証アルゴリズム、認証モード、共有の秘密のキー、再生保護のスタイル、および暗号化のタイプ（暗号化しない場合を含む）を、エンド・システムとそのホーム・サーバとの間で使うために定義する。登録の間に、ホーム登録サーバはその加入者のセキュリティ・コンテクストを加入者ディレクトリからその登録要求の中でエンド・システムによって共有されるユーザ名およびセキュリティ・パラメータ・インデックス（ＳＰＩ）を使って呼び出す。そのセキュリティ・コンテクストの中の情報が、そのセッションの間に認証、暗号化および再生保護を実施するために使われる。モビリティのセキュリティの関連付けは、加入時に無線サービス・プロバイダによって生成される。加入者が顧客サービス担当者を呼び出すこと、あるいは加入者に安全なウェブ・サイトに対してアクセスさせることのいずれかによって、加入者がこの関連付けを変更することを許すかどうかは、その無線サービス・プロバイダに任せられている。ウェブサイトのソフトウェアは無線サービス・プロバイダが、加入者が安全なウェブ・サーバからアクセスできるようにすることができるウェブ・ページをエクスポートする。この方法で、加入者はサービス・プロバイダがアクセスを可能にすることができる加入者の他の情報の他に、モビリティのセキュリティの関連付けのコンテクストを表示／変更することができる。

【０２１４】３．モデムのＭＡＣアドレス：このフィールドは加入者によって所有されているモデムのＭＡＣアドレスを含む。供給されている秘密のキーの他に、このフィールドがユーザを認証するために登録時に使われる。ＭＡＣアドレス・ベースの認証はユーザごとにオフにすることができる。ＭＡＣアドレスは登録時にホーム

登録サーバに対して通信される。

【０２１５】４．ＭＡＣアドレス認証のイネーブル：このフィールドはＭＡＣアドレス・ベースの認証がイネーブルされるか、あるいはディスエーブルされるかを決定するために使われる。イネーブルされる場合、ホーム登録サーバはそのエンド・システムのアイデンティティを検証するために、このフィールドに対して登録中のエンド・システムのＭＡＣアドレスをチェックする。ディスエーブルされている場合、チェックは行われない。

【０２１６】５．ローミング・イネーブル・フラグ：このフィールドが「イネーブル」に設定されていた場合、そのエンド・システムはフォーリン・ネットワークに対してロームすることが許される。そのフィールドが「ディスエーブル」されていた場合、そのエンド・システムはフォーリン・ネットワークに対してロームすることが許されない。

【０２１７】６．ローミング・ドメインのリスト：このフィールドはローミング・イネーブル・フラグがイネーブルに設定されている場合にだけ意味がある。このフィールドはエンド・システムがロームすることが許可されているフォーリン・ドメインのリストを含む。このリストの内容がヌルであって、ローミング・イネーブル・フラグが「イネーブル」に設定されているとき、そのエンド・システムは自由にロームすることが許される。

【０２１８】７．サービス・イネーブル／ディスエーブル・フラグ：このフィールドは加入者に対するサービスをディスエーブルするために、システム管理者が「ディスエーブル」することができる。このフィールドがディスエーブルされていた場合、その加入者はサービスに対して登録することが許される。その加入者が登録されていて、このフィールドの値が「ディスエーブル」にセットされた場合、その加入者のエンド・システムは直ちにネットワークによって切り離される。

【０２１９】８．インターネット・サービス・プロバイダの関連付け：このフィールドは加入者のインターネット・サービス・プロバイダに関する情報を含む。この情報はエンド・システムに代わってインターネット・サービス・プロバイダによる認証を実行するため、および、ＩＷＦとそのインターネット・サービス・プロバイダのＰＰＰサーバとの間にＬ２ＴＰトンネルを生成するために、ＰＰＰの登録フェーズにおいてＩＷＦによって使われる。このフィールドはその加入者のＩＳＰのアイデンティティを含む。ＩＷＦはこの情報を使って、エンド・システムに代わって認証を実行するため、およびＬ２ＴＰトンネルをセットアップするために、ＩＳＰのディレクトリにアクセスする。

【０２２０】９．加入者名およびアドレス情報：このフィールドは加入者の名前、住所、電話番号、ファックス番号、ｅメール・アドレスなどを含む。

【０２２１】ホーム・ドメイン・ディレクトリ（ＨＤ

Ｄ）はエンド・システムに代わって登録を完了するために、エンド・システムに関するパラメータを呼び出すために登録サーバによって使われる。この情報を使って、登録サーバはそのエンド・システムがホームにおいて登録しているか、あるいはそのエンド・システムがローミングしているエンド・システムであるかどうかを判定する。前者の場合、登録サーバはホーム登録サーバの役割を仮定し、エンド・システムの登録を進める。後者の場合、登録サーバはフォーリン登録サーバの役割りを仮定し、Ｒａｄｉｕｓのプロキシとして働き、このディレクトリからアイデンティティを得た実際のホーム登録サーバに対してその要求を転送する。ローミングのエンド・システムの場合、ＨＤＤに格納されるパラメータは、そのホーム登録サーバのＩＰアドレス、ホーム－フォーリン間での共有の秘密のキー、ホーム－サービスしているＩＷＦの間のトンネルのコンフィギュレーションなどを含む。ＨＤＤはＭＳＣの中に置かれている。

【０２２２】次の情報がＨＤＤに格納されている。

１．ホーム・ドメイン名：このフィールドはエンド・システムによってその登録要求の中で提供される完全にクオリファイされたホーム・ドメイン名にマッチするエントリーを求めてＨＤＤをサーチするためのキーとして使われる。

【０２２３】２．プロキシ登録要求：このフィールドは登録サーバによって、それがフォーリン登録サーバとして動作すべきかどうか、そしてそのエンド・システムの実際の登録サーバに対する登録要求を代行するかどうかを判定するために使われる。

【０２２４】３．ホーム登録サーバのＤＮＳ名：プロキシ登録要求フラグがＴＲＵＥであった場合、このフィールドは実際のホーム登録サーバのＤＮＳ名にアクセスするために使われる。それ以外の場合、このフィールドは無視される。そのＤＮＳ名はフォーリン登録サーバによってＩＰアドレスに変換される。フォーリン登録サーバはエンド・システムの登録要求を中継するためにそのＩＰアドレスを使う。

【０２２５】４．フォーリン・ドメイン名：プロキシ登録要求フラグがＴＲＵＥの場合、このフィールドはエンド・システムのホーム登録サーバに対するフォーリン・ドメイン名を識別するために使われる。それ以外の場合、このフィールドは無視される。フォーリン登録サーバはこの情報を使って、ＳＭＴＰフォーマットでのフォーリン・サーバ・マシンのｉｄ、たとえば、ｍａｃｈｉｎｅ＠ｆｑｄｎを生成する。このマシンｉｄはホーム登録サーバに対して、フォーリン登録サーバによってＲａｄｉｕｓのアクセス要求の中で送信される。

【０２２６】５．共有の秘密のキー：プロキシ要求フラグがＴＲＵＥであった場合、共有の秘密のキーはフォーリン登録サーバとホーム登録サーバとの間でそれぞれのアイデンティティを互いに認証するために使われる。そ

れ以外の場合、このフィールドは無視される。

【０２２７】６．トンネリング・プロトコルのパラメータ：このフィールドはエンド・システムに対してサービスを提供するためのトンネルを構成するためのパラメータを格納するために使われる。ホームにあるエンド・システムの場合、これは基地局とホームＩＷＦとの間、およびホームＩＷＦからＰＰＰサーバに対するトンネルのパラメータに関する情報を含む。ロームしているエンド・システムの場合、これは基地局からサービスしているＩＷＦに対するトンネリング・パラメータおよびサービスしているＩＷＦからホームＩＷＦに対するトンネリング・パラメータを含む。最小の場合、各トンネルに対して、このフィールドは使用するトンネリング・プロトコルのタイプおよびトンネリング・プロトコル固有の任意のパラメータを含む。たとえば、このフィールドはトンネリング・プロトコルＬ２ＴＰに対する識別子および、ＩＷＦとそのピアとの間でＬ２ＴＰトンネルを構成するために必要な追加のパラメータを含むことができる。

【０２２８】７．アカウンティング・サーバの関連付け。このフィールドは、ＩＷＦがエンド・システムに代わってアカウンティング・データを発生するために必要な情報を格納するために使われる。それはアカウンティング・プロトコルの名前（たとえば、ＲＡＤＩＵＳ）、そのアカウンティング・サーバのＤＮＳ名、およびＵＤＰポート番号のようなそのアカウンティング・プロトコルに固有の追加のパラメータ、Ｒａｄｉｕｓのアカウンティング・プロトコルの中でＩＷＦが使わなければならない共有の秘密のキー、チェック・ポインティングの頻度、セッション／マルチセッションｉｄを生成するためのシードなどを含む。アカウンティング・サーバのＤＮＳ名はそのアカウンティング・サーバのＩＰアドレスに変換され、それがＩＷＦに対して送信される。

【０２２９】互いにローミングの契約を結んでいる無線サービス・プロバイダの場合、認証のため、および登録プロセスを完了するためにＨＤＤが使われる。１つのエンド・システムがそのホーム・ネットワークから１つのフォーリン・ネットワークにロームする場合、そのネットワークの中のフォーリン登録サーバは、その訪問しているエンド・システムのホーム登録に関する情報を得るために、およびそのホーム・ネットワークがその訪問しているエンド・システムに対するサービスを提供する前にそのホーム・ネットワークを認証するために、そのＭＳＣの中にあるＨＤＤを参照する。

【０２３０】ホーム・ドメイン・ディレクトリの管理のためのソフトウェアは、システム管理者に対してグラフィカル・ユーザ・インターフェース（ＧＵＩ）ベースのＨＤＤマネジメント・インターフェースを提供することが好ましい。このＧＵＩを使って、システム管理者はＨＤＤの中のエントリーを表示および更新することができる。このＧＵＩは、ローミングの契約に基づいてリモートの更新を実行するためにフォーリン無線ネットワーク・サービス・プロバイダによって使われることは意図されていない。それはファイアウォールの背後において操作しているホーム無線サービス・プロバイダの信頼できる人による使用に対してのみ意図されている。

【０２３１】フォーリン・ドメイン・ディレクトリ（ＦＤＤ）はホーム・ドメイン・ディレクトリの逆の機能を提供する。ＦＤＤはホーム登録サーバによって、フォーリン・ネットワークを認証し、サービスしているＩＷＦとホームＩＷＦの間に１つのトンネルを生成するために、フォーリン登録サーバおよびフォーリン・ネットワークに関するパラメータを呼び出すために、ホーム登録サーバによって使われる。これらのパラメータはホーム－フォーリン共有の秘密のキー、ホームＩＷＦ－サービスしているＩＷＦのトンネルのコンフィギュレーションなどを含む。ＦＤＤはホーム登録サーバのＭＳＣの中に置かれていることが好ましい。ＦＤＤはロームしているエンド・システムを登録するために、ホーム登録サーバによって使われる。

【０２３２】次の情報がＦＤＤに格納される。

１．フォーリン・ドメイン名：このフィールドは、その登録要求を中継しているフォーリン登録サーバの完全にクオリファイされたドメイン名にマッチするエントリーを求めて、ＦＤＤをサーチするためのキーとして使われる。

【０２３３】２．共有の秘密のキー：これはフォーリン登録サーバとホーム登録サーバとの間でそれぞれのアイデンティティを相互に認証するために使われる共有の秘密のキーである。

【０２３４】３．ホームＩＷＦ－サービスしているＩＷＦ間のトンネリング・プロトコルのパラメータ：このフィールドはホームＩＷＦとサービスしているＩＷＦとの間のトンネルを構成するためのパラメータを格納するために使われる。最小の場合、このフィールドは使用するトンネリング・プロトコルのタイプ、およびトンネリング・プロトコル固有の任意のパラメータを含む。たとえば、このフィールドはトンネリング・プロトコルＬ２ＴＰに対する識別子および、サービスしているＩＷＦとホームＩＷＦとの間のＬ２ＴＰトンネルを構成するために必要な追加のパラメータを含むことができる。

【０２３５】４．アカウンティング・サーバの関連付け：このフィールドは、ＩＷＦがエンド・システムに代わってアカウンティング・データを発生するために必要な情報を格納するために使われる。それはアカウンティング・プロトコルの名前（たとえば、ＲＡＤＩＵＳ）、そのアカウンティング・サーバのＤＮＳ名、およびＵＤＰポート番号のようなそのアカウンティング・プロトコルに固有の追加のパラメータ、Ｒａｄｉｕｓのアカウンティング・プロトコルの中でＩＷＦが使わなければならない共有の秘密のキー、チェック・ポインティングの頻

度、セッション／マルチセッションｉｄを生成するためのシードなどを含む。アカウンティング・サーバのＤＮＳ名はそのアカウンティング・サーバのＩＰアドレスに変換され、それがフォーリン・エージェントに対して送信される。

【０２３６】互いにローミングの契約を結んでいる無線サービス・プロバイダの場合、ＦＤＤは認証を行うため、および登録プロセスを完了するために使われる。エンド・システムがそのホーム・ネットワークからフォーリン・ネットワークへロームする場合、そのホーム・ネットワークの中の登録サーバはそのエンド・システムに対してサービスを提供するフォーリン・ネットワークの情報を得て認証するために、そのＭＳＣの中のＦＤＤを参照する。

【０２３７】フォーリン・ドメイン・ディレクトリ管理ソフトウェアは、システム管理者に対してグラフィカル・ユーザ・インターフェース（ＧＵＩ）ベースのＦＤＤマネジメント・インターフェースを提供する。このＧＵＩを使って、システム管理者はＦＤＤの中のエントリーを表示および更新することができる。このＧＵＩは、ローミングの契約に基づいてリモートの更新を実行するためにフォーリン無線ネットワーク・サービス・プロバイダによって使われることは意図されていない。それはファイアウォールの背後において操作しているホーム無線サービス・プロバイダの信頼できる人による使用に対してのみ意図されている。

【０２３８】インターネット・サービス・プロバイダのディレクトリ（ＩＳＰＤ）は加入者がそのネットワークを使ってそれぞれのＩＳＰにアクセスすることができるように、無線サービス・プロバイダとサービス契約を結んでいるＩＳＰとの接続性を管理するために、ホームＩＷＦによって使われる。各加入者に対して、加入者ディレクトリにはその加入者のＩＳＰに対する１つのエントリーがある。このフィールドはＩＳＰＤの中の１つのエントリーをポイントする。ホームＩＷＦはこの情報を使って、加入者に代わってＩＳＰに対するコネクションをセットアップする。

【０２３９】ネットワーク・アーキテクチャはローミングをサポートする。無線サービス・プロバイダ間でのローミングが正常に動作するためには、そのアーキテクチャは無線サービス・プロバイダ間でのローミング契約のセットアップをサポートしなければならない。これは２つのこと、すなわち、（１）無線サービス・プロバイダ間にまたがるシステム・ディレクトリの更新および、（２）サービス・プロバイダ間での料金請求の精算を意味する。

【０２４０】加入者がインターネット・サービス・プロバイダにアクセスできるようにするために、このアーキテクチャはインターネット・サービス・プロバイダとのローミング契約をサポートする。これはそのアーキテクチャがＩＳＰのＰＰＰサーバ（すなわち、ＰＰＰ、Ｌ２ＴＰおよびＲａｄｉｕｓのなどの業界標準のプロトコルをサポートする）との間でデータを送受信しなければならないことを意味する。それはまた、そのアーキテクチャがＩＳＰのアクセスに対するディレクトリの更新およびＩＳＰとの料金請求の精算を扱うことを意味する。

【０２４１】ローミングの契約が２つの無線サービス・プロバイダ間で締結されているとき、両方のプロバイダは他のネットワークからそれぞれのネットワークを訪問して来ているエンド・システムに対する認証および登録の機能をサポートするために、それぞれのホームおよびフォーリンのドメイン・ディレクトリを更新しなければならない。最小の場合、本実施形態のアーキテクチャは手動でのディレクトリ更新をサポートする。ローミング契約が２つの無線サービス・プロバイダ間で締結されているとき、その２つのパーティはそれぞれのホームおよびフォーリンのドメイン・ディレクトリを埋めるための情報を交換する。そのディレクトリの実際の更新はそれぞれのサービス・プロバイダの職員によって手動で行われる。後で、そのホームおよびフォーリンのドメイン・ディレクトリの中の情報を更新する必要があった場合、その契約のために２つのパーティは更新される情報を交換してから、それぞれの更新をディレクトリに対して手動で適用する。

【０２４２】他の実施形態においては、インターネット・サービス・プロバイダ間でのローミングをイネーブルするため、および、ＩＳＰがローミングの関係を自動的に管理して発見することができるようにするために、ディレクトリ管理ソフトウェアはＩＥＴＦにおいて開発中の標準を組み込む。これによって手動でのディレクトリ管理が不要となる。ネットワーク・システムはローミングの関係を自動的に伝播し、そしてそれらを発見し、訪問しているエンド・システムを認証して登録する。

【０２４３】最小の場合、ネットワーク・アーキテクチャはアカウンティング・データを処理し、それを格納し、そのデータを無線サービス・プロバイダの料金請求システムが利用できるようにするだけである。ローミングに対する料金請求の精算を扱うことはその料金請求システムに任されている。

【０２４４】他の実施形態においては、インターネット・サービス・プロバイダ間でのアカウンティング・レコードの配分を扱うために、ロームしているエンド・システムに対する料金の精算をＩＳＰが行うことができるようにするために、ＩＥＦＴにおいて開発中の標準が組み込まれている。

【０２４５】システム・ソフトウェアはホームＩＷＦとＩＳＰまたはイントラネットのＰＰＰサーバとの間にＬ２ＴＰをサポートすることによって、ＩＳＰおよびプライベート・イントラネットに対するアクセスをサポートする。インターネット・サービス・プロバイダのディレ

クトリは、これらのトンネルを生成するためにＩＷＦにとって役立つ情報を含んでいる。無線サービス・プロバイダとインターネット・サービス・プロバイダ間のアクセス契約が締結されている場合、このディレクトリは無線サービス・プロバイダの職員によって手動で更新される。無線サービス・プロバイダとインターネット・サービス・プロバイダとの間のアクセスの関係の自動更新および発見は現在考慮中であり、そしてインターネットの標準が進化するにつれて実装される。インターネット・サービス・プロバイダにアクセスしている間に、加入者は２つの料金請求を受け取る。１つは無線ネットワークの使用に対する無線サービス・プロバイダからのものであり、もう１つはインターネット・サービス・プロバイダからのものである。２つのタイプの料金を組み合わせる共通の料金請求は最小構成の具体例のソフトウェアによっては扱われないが、加入者がＩＳＰと無線サービス・プロバイダとの間のローミングの契約に基づいて共通の料金請求を受け取ることができるように、料金の精算に対するインターネットの標準が進化する際に、そのソフトウェアがそれを利用することが考えられる。

【０２４６】このシステムは、ネットワーク要素を管理するための要素管理システムを含む。要素マネージャから、システム管理者はコンフィギュレーション、性能および故障／アラームの管理機能を実行する。要素管理のアプリケーションはウェブ・ブラウザのトップにおいて実行される。ウェブ・ブラウザを使って、システム管理者はＴＣＰ／ＩＰのアクセスを備えている任意の場所からそのネットワークを管理する。また、要素マネージャは上位レベルのマネージャに対するエージェントの役割りを果たす。この役割りにおいて、それはアラームおよび故障監視のためにＳＮＭＰ　ＭＩＢをエクスポートする。

【０２４７】上位レベルのＳＮＭＰマネージャには、ＳＮＭＰのトラップを経由してアラーム状態が通知される。上位レベルのＳＮＭＰマネージャはネットワークの健康状態およびそのステータスを求めて要素マネージャのＭＩＢを定期的にポールする。上位レベルのマネージャにおけるシステム管理の職員はネットワークおよびその現在のアラーム状態を表しているアイコンを見ることができる。そのネットワーク要素のアイコンをポイントしてクリックすることによって、システム管理の職員はウェブ・ブラウザを使って要素管理のアプリケーションを実行し、そしてより詳細の管理機能を実行する。

【０２４８】ネットワーク内では、物理的および論理的ネットワーク要素の管理が、ＳＮＭＰプロトコルと内部管理のアプリケーション・プログラミング・インターフェースとの組合せを使って実行される。要素マネージャの中のアプリケーションはＳＮＭＰまたは他のマネージメントＡＰＩを使ってネットワーク管理機能を実行する。

【０２４９】アーキテクチャ的には、要素マネジメントのシステムは２つの明確に異なる機能要素の組を含む。第１の組の機能要素は、コンフィギュレーション・データ・サーバ、パーフォーマンス・データ・モニタおよびヘルス／ステータス・モニタおよびネットワーク要素回復ソフトウェアを含んでいて、ＲＡＩＤディスクを装備したＨＡサーバ上で実行する。マネジメントのアプリケーションを含んでいる第２の組の機能要素は、専用の、非ＨＡマネジメント・システム上で実行する。要素マネージャ・システムが動作しなくなった場合でも、ネットワーク要素は実行し続けることができ、そしてアラームをレポートし、そして故障状態から回復することさえできる。しかし、すべてのマネジメント・アプリケーションは非ＨＡの要素マネージャの中で実行するので、要素マネージャがダウンした場合、その要素マネージャが動作するようになるまで、人間の介入を必要とする回復のアクションは不可能である。

【０２５０】基地局の中の無線ハブ（ＷＨ）は、通常は、無線サービス・プロバイダ（ＷＳＰ）によって所有されており、そしてそれらはポイント・ツー・ポイントのリンク、イントラネット、またはインターネットのいずれかを経由してそのＷＳＰの登録サーバ（ＲＳ）に対して接続されている。ＷＳＰの登録サーバは、通常は、或る種の登録機能を実行するためにプロセッサ上で実行しているソフトウェア・モジュールである。インターワーキング機能ユニット（ＩＷＦユニット）は、通常は、或る種のインターフェース機能を実行するためにプロセッサ上で実行しているソフトウェア・モジュールである。ＩＷＦユニットは、通常は、イントラネット／ＷＡＮを経由して登録サーバに接続されており、ＩＷＦユニットは、通常は、ＷＳＰによって所有されている。しかし、ＩＷＦユニットは登録サーバと同じＬＡＮの内部に置かれている必要はない。通常、アカウンティングおよびディレクトリのサーバ（これもプロセッサ上で実行しているソフトウェア・モジュール）はサービス・プロバイダのデータ・センター（たとえば、各種のサーバおよび他のソフトウェア・モジュールをホストする１つまたはそれ以上のプロセッサを含んでいるセンター）の中のＬＡＮを経由して登録サーバに接続されている。エンド・システムからのトラヒックはルータ（ＬＡＮに接続されている）を経由してパブリック・インターネットまたはＩＳＰのイントラネットに対して回送される。フォーリンＷＳＰのネットワークに置かれている登録サーバはフォーリン登録サーバ（ＦＲＳ）と呼ばれ、そしてエンド・システムのホーム・ネットワーク（モバイルがそのサービスをここで購入する）に置かれている登録サーバはホーム登録サーバ（ＨＲＳ）と呼ばれる。ホーム・ネットワークの中のインターワーキング機能ユニットはホームＩＷＦと呼ばれ、一方、フォーリン・ネットワーク（すなわち、エンド・システムが訪問しているネットワ

ーク）の中のインターワーキング機能はサービスしているＩＷＦと呼ばれる。

【０２５１】固定型の無線サービス（すなわち、移動していないエンド・システム）の場合、エンド・システムはホーム・ネットワークから（たとえば、ホームにおけるサービス）、あるいはフォーリン・ネットワークから（たとえば、ローミング・サービス）ホーム・ネットワーク上のサービスに対して登録することができる。エンド・システムはアクセス・ポイントを経由して、その無線ハブの中のエージェント（たとえば、ソフトウェアで実装されているエージェント機能）によって送信される公示を受信する。ネットワーク層の登録以外にＭＡＣ層の登録も行われる。これらは効率をよくするために一緒に組み合わせることができる。

【０２５２】ホームにいるエンド・システムの場合（図２３）、ネットワーク層の登録（ローカル登録など）はエンド・システムが現在付加されている無線ハブをホーム登録サーバに対して知られるようにする。エンド・システムのホーム・ネットワークの中のＩＷＦはアンカー、すなわち、ホームＩＷＦとなる。したがって、エンド・システムとの間のＰＰＰフレームは無線ハブを経由してホーム・ネットワークの中のホームＩＷＦへ転送される。エンド・システムがホームにある場合、そのホームＩＷＦがＸＴｕｎｎｅｌプロトコルを経由してその無線ハブに接続される。

【０２５３】ローミングの無線サービス（図２４）の場合、フォーリン登録サーバは登録フェーズの間にロームしているエンド・システムのホーム・ネットワークのアイデンティティを知る。この情報を使ってフォーリン登録サーバはそのエンド・システムを認証して登録するためにホーム登録サーバと通信する。次に、フォーリン登録サーバは１つのサービスしているＩＷＦを割り当て、そしてＩ－ＸＴｕｎｎｅｌプロトコルのコネクションが、そのホームＩＷＦとサービスしているＩＷＦとの間にエンド・システムをロームするために設立される。サービスしているＩＷＦは無線ハブとホームＩＷＦとの間でフレームを中継する。そのホームＩＷＦから、その同じＩＷＦの中に駐在している可能性のあるＰＰＰサーバ（すなわち、ポイント・ツー・ポイント・プロトコル・サーバ）に対してデータが送信される。しかし、そのデータが自分自身のＰＰＰサーバを備えている企業のイントラネットまたはＩＳＰのイントラネットに送られる場合、そのデータはＬ２ＴＰプロトコルを経由して別のＰＰＰサーバに対して送信される。その別のサーバは、通常は、その無線サービス・プロバイダとは異なるインターネット・サービス・プロバイダによって所有され、稼働されている。そのセッションの間中、ホームＩＷＦおよびＰＰＰサーバのロケーションは固定のままである。ＭＡＣ層の登録は、ＭＡＣ層およびネットワーク層の登録のための別々の通信のオーバヘッドについて経済化するために、ネットワーク登録と組み合わせることができる。しかし、そのＷＳＰの装置が純粋のＩＥＴＦのモバイルＩＰをサポートする他の無線ネットワークと相互運用されるように、これらの登録プロセスを組み合わせない方が有利である場合がある。

【０２５４】登録は３つのテーブルをセットアップする。テーブル１は各アクセス・ポイントに関連付けられており、テーブル１は各コネクション（たとえば、各エンド・システム）を、コネクションＩＤ（ＣＩＤ）によって識別し、そしてそのコネクションＩＤを特定の無線モデム（WM）のアドレス（すなわち、エンド・システムまたはエンド・システムのアドレス）と関連付ける。テーブル２は各無線ハブ（WH）と関連付けられており、そしてテーブル２は各コネクションＩＤを対応している無線モデムのアドレス、アクセス・ポイントおよびＸＴｕｎｎｅｌのＩＤ（ＸＩＤ）と関連付ける。テーブル３は各インターワーキング機能（ＩＷＦ）に関連付けられ、そしてテーブル３は各コネクションＩＤを対応している無線モデムのアドレス、無線ハブのアドレス、ＸＴｕｎｎｅｌのＩＤおよびＩＰポート（ＩＰ／ｐｏｒｔ）に関連付ける。これらのテーブルのための記述されるエントリーは、モビリティ管理の説明をサポートする関連のエントリーだけを含むように説明される。実際には、それ以外に含められる必要がある重要な他のフィールドもある。

【０２５５】

【表１】

61

表１：　ＡＰにおけるコネクション・テーブル

ＣＩＤ	WM
Ｃ１	WM１
Ｃ２	WM１
Ｃ３	WM２

表２：　WHにおけるコネクション・テーブル

ＣＩＤ	WM	ＡＰ	ＸＩＤ
Ｃ１	WM１	ＡＰ１	５
Ｃ２	WM１	ＡＰ１	５
Ｃ１	WM２	ＡＰ１	６
Ｃ１	WM３	ＡＰ２	７

表３：　ＩＷＦにおけるコネクション・テーブル

ＣＩＤ	WM	WH	ＸＩＤ	IP/Port
Ｃ１	WM１	WH１	５	IP1/P1
Ｃ２	WM１	WH１	５	IP1/P2
Ｃ１	WM２	WH１	６	IP2/P3
Ｃ１	WM３	WH１	７	IP3/P1
Ｃ５	WM５	WH２	８	IP4/P1

【０２５６】ロームしているユーザと同様に、ネットワーク内のホームにあるダイヤルアップ・ユーザに対するプロトコル・スタックが図２５～図２８に示されている。図２５はホームにいる固定型の（すなわち、移動していない）エンド・システムによって直接のインターネット・アクセスのために使われるプロトコル・スタックを示しており、ＰＰＰプロトコルのメッセージはホームＩＷＦ（通常は、線ハブと同じ場所に置かれている）においてターミネートし、ホームＩＷＦはＩＰルータとの間でメッセージを中継し、そこからパブリック・インターネットに対して中継する。図２６はホームにいる固定型の（すなわち、移動していない）エンド・システムによってリモートのイントラネット（すなわち、私企業のネットまたはＩＳＰ）にアクセスするために使われるプロトコル・スタックを示しており、ＰＰＰプロトコル・メッセージはホームＩＷＦ（無線ハブと通常は同じ場所にある）を通して私企業のイントラネットまたはＩＳＰのＰＰＰサーバに対して中継する。図２７はロームしているが固定されている（すなわち、移動していない）エンド・システムまたは移動しているエンド・システムによって直接にインターネットにアクセスするために使われるプロトコル・スタックを示しており、ＰＰＰプロトコルはホームＩＷＦ（通常は、そのホーム・ネットワークの移動交換センターにある）においてターミネートし、そのホームＩＷＦはＩＰルータとの間でメッセージを中継する。図２７において、メッセージのトラヒックがホームＩＷＦ以外にサービスしているＩＷＦ（通常は、無線ハブと同じ場所にある）をどのように通過するかに留意されたい。図２８はロームしているが、固定されている（すなわち、移動していない）エンド・システムまたは移動しているエンド・システムによってリモートのイントラネット（すなわち、私企業のネットまたはＩＳＰ）にアクセスするために使われるプロトコル・スタックを示しており、ＰＰＰプロトコル・メッセージはホームＩＷＦ（通常は、ホーム・ネットワークの移動交換センターにある）を通して私企業のイントラネットまたはＩＳＰのＰＰＰサーバに中継される。図２８において、メッセージ・トラヒックがホームＩＷＦ以外に、サービスしているＩＷＦ（通常は、無線ハブと同じ場所にある）をどのように通過するかに留意されたい。サービスしているＩＷＦおよび無線ハブがコンピュータの同じネストに共存しているか、あるいは同じコンピュータにプログラムされているとき、そのサービスしているＩＷＦと無線ハブとの間にＸＴｕｎｎｅｌプロトコルを使ったトンネルを設立する必要はない。

62

【０２５７】これらのプロトコル・スタックに対する等価な変形版（たとえば、ホームにいるモバイルに対して、ＲＬＰをサービスしているＩＷＦまたはホームＩＷＦにおいてではなく、無線ハブにおいてターミネートさせることができる）も考えられる。ＩＷＦが無線ハブから離れた場所にある場合、そしてパケットを、ＩＷＦと無線ハブとの間の損失の多いＩＰネットワーク上で搬送される可能性がある場合、ＲＬＰプロトコルを無線ハブにおいてターミネートすることが好ましいことになる。もう１つの変形版は無線ハブとＩＷＦとの間のＸＴｕｎｎｅｌがＵＤＰ／ＩＰのトップに作られる必要がないものである。ＸＴｕｎｎｅｌはフレーム・リレー／ＡＴＭのリンク層を使って構築することができる。しかし、ＵＤＰ／ＩＰを使うことによって、無線ハブおよびＩＷＦソフトウェアを１つのネットワークから別のネットワークへ容易に移動させることができる。

【０２５８】さらに、ＰＰＰプロトコルは無線モデムにおいてターミネートされ、そしてイーサネット接続経由で１つまたはそれ以上のエンド・システムに対して送信されるようにすることができる。図２９に示されているように、無線モデム３００はＰＰＰプロトコル情報を受信し、そのＰＰＰペイロードをイーサネット・フレームにカプセル化して、インターネット・コネクション３０２経由で少なくとも１つのエンド・システム３０４および３０６に対して転送されるようにする。

【０２５９】ＸＷＤ　ＭＡＣをカプセル化するためにＤＩＸイーサネットを使うことができるが、このシステムはそれに限定されない。ＸＷＤ制御フレームに対するイーサネット・フレームのフォーマットが図３０に示されている。イーサネットのヘッダは宛先アドレス、ソース・アドレスおよびイーサネットのタイプ・フィールドを

含む。宛先アドレスのフィールドは、プリミティブが送信されているＭＡＣエンティティのイーサネット・アドレスを含む。ＭＡＣのユーザによって呼び出されるＭＡＣプリミティブの場合、このフィールドはそのＭＡＣユーザのイーサネット・アドレスを含むことになる。ブロードキャスト・プリミティブの場合、このアドレスはイーサネットのブロードキャスト・アドレスとなる。ソース・アドレス・フィールドはそのプリミティブを呼び出しているＭＡＣエンティティのイーサネット・アドレスを含む。イーサネット・タイプ・フィールドはＸＷＤに対するイーサネット・タイプを含む。可能な値は、制御フレームの場合はＸＷＤ＿Ｃｏｎｔｒｏｌであり、データ・フレームの場合はＸＷＤ＿Ｄａｔａである。これらの値はこれまでに標準化されているすべてのイーサネット・タイプとは異なるものでなければならず、そして制御のオーソリティによって登録されていなければならない。

【０２６０】次に、イーサネット・フレームにはＸＷＤのヘッダ・フィールドがある。このＸＷＤヘッダは長さを１６ビットとすることができ、そしてＸＷＤの制御フレームに対してのみ存在する。そのフィールドが図３１に示されている。このイーサネット・フレームもプロトコル・ヘッダ、ＰＰＰのペイロード・フィールドおよびＸＷＤのＭＡＣフィールドを含んでいる。イーサネットのカプセル化を使っているプリミティブに対するヘッダの値が以下の表４に示されている。

【０２６１】

【表２】

ﾌﾟﾘﾐﾃｨﾌﾞ名	宛先ｱﾄﾞﾚｽ	ｿｰｽ・ｱﾄﾞﾚｽ	ｲｰｻﾈｯﾄ・ﾀｲﾌﾟ	XWD MACの ﾌﾟﾘﾐﾃｨﾌﾞ
M_Discobver. Req	ﾌﾞﾛｰﾄﾞｷｬｽﾄまたはﾕﾆｷｬｽﾄのMACﾌﾟﾛﾊﾞｲﾀﾞ	MACﾕｰｻﾞ	XWD_Control	0
M_Discobver. Cnf	MACﾕｰｻﾞ	MACﾌﾟﾛﾊﾞｲﾀ	XWD_Control	1
M_OpenSap. Req	MACﾌﾟﾛﾊﾞｲﾀﾞ	MACﾕｰｻﾞ	XWD_Control	2
M_OpenSap. Cnf	MACﾕｰｻﾞ	MACﾌﾟﾛﾊﾞｲﾀ	XWD_Control	3
M_CloseSap. Req	MACﾌﾟﾛﾊﾞｲﾀﾞ	MACﾕｰｻﾞ	XWD_Control	4
M_CloseSap. Cnf	MACﾕｰｻﾞ	MACﾌﾟﾛﾊﾞｲﾀ	XWD_Control	5
M_EchoSap. Req	MACﾕｰｻﾞ	MACﾌﾟﾛﾊﾞｲﾀ	XWD_Control	6
M_EchoSap. Cnf	MACﾌﾟﾛﾊﾞｲﾀﾞ	MACﾕｰｻﾞ	XWD_Control	7
M_Connect. Req	MACﾌﾟﾛﾊﾞｲﾀﾞ（ﾓﾃﾞﾑ専用）	MACﾕｰｻﾞ（ｴﾝﾄﾞ・ｼｽﾃﾑ専用）	XWD_Control	8
M_Connect. Ind	MACﾕｰｻﾞ（無線ﾊﾌﾞ専用）	MACﾌﾟﾛﾊﾞｲﾀﾞ（AP専用）	XWD_Control	9
M_Connect. Rsp	MACﾌﾟﾛﾊﾞｲﾀﾞ（AP専用）	MACﾕｰｻﾞ（無線ﾊﾌﾞ専用）	XWD_Control	10
M_Connect. Cnf	MACﾕｰｻﾞ（ｴﾝﾄﾞ・ｼｽﾃﾑ専用）	MACﾌﾟﾛﾊﾞｲﾀﾞ（ﾓﾃﾞﾑ専用）	XWD_Control	11
M_Disconnect. Req	MACﾌﾟﾛﾊﾞｲﾀﾞ	MACﾕｰｻﾞ	XWD_Control	12

【０２６２】別の代替例において、ＰＰＰプロトコルは無線ルータの中でターミネートすることができ、そしてローカル・エリア・ネットワーク（ＬＡＮ）に接続されている少なくとも１つのエンド・システムに対して送信される。図３２に示されているように、無線ルータ３５０は無線モデム３５２を経由してＰＰＰプロトコル情報を受信する。ルータ３５４は無線モデム３５２からＰＰＰ情報を受信し、そのＰＰＰ情報を、ＬＡＮリンク３６２経由でエンド・システム３５６、３５８、３６０のうちの少なくとも１つに対して送信する。

【０２６３】４種類のハンドオフ・シナリオが発生する可能性があり、それらは、（ｉ）ローカル・モビリティ、（ii）マイクロ・モビリティ、（iii）マクロ・モビリティ、および（ｉｖ）グローバル・モビリティと命名される。４つのシナリオのすべてにおいて（本発明の１つの実施形態の中で）、ルートの最適化のオプションは考慮されず、ホーム登録サーバおよびＩＳＰのＰＰＰサーバのロケーションは変化しないようになっている。

ルートの最適化を伴うシステムの別の実施形態においては、ＩＳＰのＰＰＰサーバは変化する可能性がある。しかし、このことについては以下に説明される。さらに、最初の３つのシナリオにおいては、フォーリン登録サーバおよびＩＷＦのロケーションは変化しない。

【０２６４】提案されているＩＥＴＦのモバイルＩＰの標準は、エンド・システムが、自分が付加されているＩＰサブネットを変更するときは常に、それはそのホームサブネットの中のホーム・エージェントに対して登録要求メッセージを送信する必要がある。このメッセージはケア・オブ・アドレスを搬送し、そのエンド・システムはそのアドレスで新しいサブネットの中でアクセスすることができる。たとえば、ＩＳＰからエンド・システムに対してトラヒックが送信されると、ホーム・エージェントはエンド・システムへ向かっているトラヒックを、それがホーム・サブネットに到着した際に横取りし、次にそのトラヒックをそのケア・オブ・アドレスに対して転送する。ケア・オブ・アドレスはフォーリン・サブネットの中の特定のフォーリン・エージェントを識別する。エンド・システムのフォーリン・エージェントはそのエンド・システム自身の中に駐在すること、あるいはトラヒックを順にそのエンド・システムに対して転送する別のノード（すなわち、プロキシ登録エージェント）の中に駐在することが可能である。モバイルのＩＰハンドオフは、エンド・システムのエージェント、エンド・システムのホーム・エージェントおよび潜在的にそれに対応しているホスト（ＣＨ）（ルート最適化オプション付き）の間で制御メッセージの交換が必要である。

【０２６５】提案されているＩＥＴＦのモバイルＩＰ標準は、大規模なインターネットワークにおけるすべての移動に対するレイテンシーおよびスケーラビリティの目標を満足することが難しいことが分かる。しかし、本発明の階層的なモビリティ管理はそのような目標を満足する。小さな移動（たとえば、アクセス・ポイントの変更）の場合、ＭＡＣ層の再登録だけが必要である。比較的大きな移動の場合は、ネットワーク層の再登録が行われる。本発明の階層的モビリティ管理はＩＥＴＦの提案されているモバイルＩＰ標準において使われているフラット構造とは異なり、またＣＰＤＰ（セルラー・ディジタル・パケット・データのフォーラムによって保証されている標準に基づくもの）などのセルラー・システムにおいて使われている、サービスしている／アンカーのインターワーキング機能とも異なっている。

【０２６６】図３３に示されているように、ローカル・モビリティのハンドオフは、同じ無線ハブに所属しているＡＰ間でのエンド・システム（モバイル・ノードとしてＭＮで示されている）の移動を扱う。したがって、ＭＡＣ層の再登録だけが必要である。エンド・システムは新しいＡＰから無線ハブの公示を受信し、そしてその新しいＡＰに対してアドレスされている登録要求で応答する。

【０２６７】新しいＡＰ（すなわち、そのエンド・システムからの登録要求を受信するＡＰ）は自分のコネクション・テーブルに新しいエントリーを生成し、その登録メッセージをその無線ハブに対して中継する。ローカル・モビリティのハンドオフにおいては、無線ハブは変化しない。無線ハブはエンド・システムの登録要求をＭＡＣレベルの登録要求であるとして認証し、自分のコネクション・テーブルを、その新しいＡＰに対するコネクションを反映するように更新する。次に、前のＡＰは自分のコネクション・テーブルからそのコネクション・エントリーを削除する。前のＡＰが前のエントリーを削除することができる方法が少なくとも３つある。それらは、（ｉ）タイムアウト時、（ii）新しいＡＰから無線ハブへの中継されたＭＡＣ層関連付けメッセージのコピーを受信したとき（この中継メッセージがブロードキャスト・メッセージである場合）、（iii）そのエントリーを削除する必要があることを無線ハブから通知されたときである。

【０２６８】図３４に示されているように、マイクロ・モビリティのハンドオフは同じ登録サーバに属していて、エンド・システムが依然として既存のサービスしているＩＷＦによってサービスされ得る無線ハブ間でのエンド・システム（モバイル・ノードとしてＭＮで示されている）の移動を扱う。公示が新しい無線ハブから（新しいＡＰを通して）受信されると、エンド・システムは登録を要求するためのメッセージを登録サーバに対して送信する。その登録要求は新しいＡＰから新しい無線ハブへ中継されて登録サーバへ送られる。

【０２６９】既存のＩＷＦがまだ使えることを判定すると、登録サーバは既存のＩＷＦを要求するために作られたＸＴｕｎｎｅｌ要求メッセージを送信し、新しい無線ハブに対してＸＴｕｎｎｅｌを作る。その後、登録サーバは前の無線ハブとの既存のＸＴｕｎｎｅｌを破棄することを既存のＩＷＦに要求するためのＸＴｕｎｎｅｌ破棄要求メッセージを送信する。その作成および破棄のＸＴｕｎｎｅｌ要求メッセージを１つのメッセージの中に組み合わせることができる。フォーリン登録サーバは、サービスしているＩＷＦまたはホームＩＷＦのいずれもＩＷＦの変更がないので、ホーム登録サーバに対してその登録メッセージを転送しない。

【０２７０】肯定のＸＴｕｎｎｅｌ作成応答および肯定のＸＴｕｎｎｅｌ破棄応答を受信すると、登録サーバは登録応答をエンド・システムに対して送信する。登録応答がその新しい無線ハブに到着すると、新しい無線ハブにあるコネクション・テーブルがその新しいＡＰに対するコネクションを反映するように更新される。新しいＡＰは、新しい無線ハブからメッセージを受信した後、自分のＭＡＣフィルタ・アドレス・テーブルおよびコネクション・テーブルを更新し、登録応答がエンド・システ

ムに対して転送される。

【０２７１】登録サーバは前の無線ハブに対して解放メッセージを送信する。前の無線ハブがその解放メッセージを受信すると、それは自分のコネクション・テーブルおよびＭＡＣフィルタ・アドレス・テーブルおよび前のＡＰのコネクション・テーブルを更新する。

【０２７２】図３５に示されているように、マクロ・モビリティのハンドオフの場合、フォーリン・ネットワーク内のサービスしているＩＷＦの変更が必要であるが、登録サーバの変更が必要でない無線ハブ間の移動を扱う。新しい無線ハブから（新しいＡＰを通して）公示が受信されると、エンド・システムは新しいネットワーク層の登録を要求するためのメッセージを登録サーバに対して送信する。その登録要求は新しいＡＰから新しい無線ハブに対して中継されて登録サーバへ送られる。

【０２７３】登録サーバは、エンド・システムが現在の登録サーバのネットワークに所属していないとき、それがフォーリン登録サーバであることを認識する。このフォーリン登録サーバはフォーリン・ディレクトリ・サーバ（大型のイエロー・ページのような）に対して、１つの要求（Ｒａｄｉｕｓのアクセス要求（ＲＡ要求）が好ましい）を使うことによって、ホーム登録サーバのアイデンティティを求め、そして適切なＩＷＦをサービスしているＩＷＦであるとして割り当て、そして１つの要求（Ｒａｄｉｕｓのアクセス要求（ＲＡ要求）であることが好ましい）を通して、ホーム登録サーバに対して登録要求を転送し、その新しく選択されたＩＷＦについてホーム登録サーバに知らせる。

【０２７４】ホーム登録サーバはホームディレクトリ・サーバに対して１つの要求（Ｒａｄｉｕｓのアクセス要求（ＲＡ要求）であることが好ましい）を使うことによって、その登録要求を認証する。その要求を認証し、既存のホームＩＷＦがまだ使えることを知ると、ホーム登録サーバはその新しく割り当てられたサービスしているＩＷＦに対して新しいＩ－ＸＴｕｎｎｅｌを作るようにホームＩＷＦに指示し、そして前のサービスしているＩＷＦに対して存在しているＩ－ＸＴｕｎｎｅｌを破棄するように指示する。肯定のＩ－ＸＴｕｎｎｅｌ作成応答および肯定のＩ－ＸＴｕｎｎｅｌ破棄応答をホームＩＷＦから受信すると、ホーム登録サーバは登録応答をフォーリン登録サーバに対して送信する。

【０２７５】次に、フォーリン登録サーバはその新しい無線ハブに対するＸＴｕｎｎｅｌを作るようその新しく割り当てられたＩＷＦに指示する。肯定のＸＴｕｎｎｅｌ作成応答を受信すると、フォーリン登録サーバは前の無線ハブに対するＸＴｕｎｎｅｌを破棄するよう、前のＩＷＦに指示する。肯定のＸＴｕｎｎｅｌの作成応答および肯定のＸＴｕｎｎｅｌ破棄応答を受信すると、フォーリン登録サーバは登録応答をエンド・システムに対して送信する。

【０２７６】登録応答が新しい無線ハブに到着すると、その新しい無線ハブにあるコネクション・テーブルがその新しいＡＰに対するコネクションを反映するように更新される。新しいＡＰは新しい無線ハブからのメッセージを受信した後、自分のＭＡＣフィルタ・アドレス・テーブルおよびコネクション・テーブルを更新し、登録応答がエンド・システムに対して転送される。

【０２７７】登録サーバは前の無線ハブに対して解放メッセージを送信する。その解放メッセージを受信すると、前の無線ハブは自分のコネクション・テーブルおよびＭＡＣフィルタ・アドレス・テーブルを更新し、また、前のＡＰは前の無線ハブからメッセージを受信した後、自分のＭＡＣフィルタ・アドレス・テーブルおよびコネクション・テーブルを更新する。

【０２７８】グローバル・モビリティのハンドオフの場合、登録サーバの変更を必要とする無線ハブ間の移動を扱う。図３６はホームＩＷＦが変化しない場合のグローバル・モビリティのハンドオフを示し、そして図３７はホームＩＷＦが変化する場合のグローバル・モビリティのハンドオフを示している。新しいフォーリン・ネットワークの中の新しい無線ハブから（新しいＡＰを通じて）公示が受信されると、エンド・システムはネットワーク層の登録を要求するためのメッセージをその新しいフォーリン登録サーバに対して送信する。その登録要求は新しいＡＰから新しい無線ハブへ中継されて新しいフォーリン登録サーバへ送られる。

【０２７９】登録サーバは、エンド・システムが現在の登録サーバのネットワークに所属していないとき、それが新しいフォーリン登録サーバであることを認識する。このフォーリン登録サーバはフォーリン・ディレクトリ・サーバ（大型のイエロー・ページのような）に対して、１つの要求（Ｒａｄｉｕｓのアクセス要求（ＲＡ要求）であることが好ましい）を使うことによって、ホーム登録サーバのアイデンティティを求め、そして１つの適切なＩＷＦを、サービスしているＩＷＦであるとして割り当て、そして１つの要求（Ｒａｄｉｕｓのアクセス要求（ＲＡ要求）であることが好ましい）を通して、ホーム登録サーバに対して登録要求を転送し、その新しく選択されたＩＷＦについてホーム登録サーバに知らせる。

【０２８０】ホーム登録サーバはホームディレクトリ・サーバに対して、１つの要求（Ｒａｄｉｕｓのアクセス要求（ＲＡ要求）であることが好ましい）を使うことによって、その登録要求を認証する。その要求を認証し、既存のホームＩＷＦがまだ使えることを知ると（図３６）、ホーム登録サーバはその新しい登録サーバによって新しく割り当てられたサービスしているＩＷＦに対する新しいＩ－ＸＴｕｎｎｅｌを作るよう、ホームＩＷＦに指示する。また、ホーム登録サーバは前のフォーリン登録サーバに対して登録解除のメッセージをも送信し、

そして前のフォーリン・ネットワークの存在しているサービスしているＩＷＦに対する既存のＩ－ＸＴｕｎｎｅｌを破棄するよう、ホームＩＷＦに指示する。肯定のＩ－ＸＴｕｎｎｅｌ作成応答および肯定のＩ－ＸＴｕｎｎｅｌ破棄応答をホームＩＷＦから受信すると、ホーム登録サーバは登録応答を新しいフォーリン登録サーバに対して送信する。

【０２８１】次に、新しいフォーリン登録サーバはその新しい無線ハブに対するＸＴｕｎｎｅｌを作るよう、その新しく割り当てられたＩＷＦに指示する。肯定のＸＴｕｎｎｅｌ作成応答を受信すると、フォーリン登録サーバは登録応答をエンド・システムに対して送信する。登録応答が新しい無線ハブに到着するとその新しい無線ハブにあるコネクション・テーブルが、新しいＡＰに対するそのコネクションを反映するように更新される。新しいＡＰは新しい無線ハブからメッセージを受信した後、自分のＭＡＣフィルタ・アドレス・テーブルおよびコネクション・テーブルを更新し、登録応答がエンド・システムに対して転送される。

【０２８２】前のフォーリン登録サーバは前の無線ハブに対するＸＴｕｎｎｅｌを破棄するよう、前のＩＷＦに指示する。肯定のＸＴｕｎｎｅｌ破棄応答を受信したとき、あるいはＸＴｕｎｎｅｌの破棄要求と同時に、前のフォーリン登録サーバは前の無線ハブに対して解放メッセージを送信する。その解放メッセージを受信すると、前の無線ハブは自分のコネクション・テーブルおよびＭＡＣフィルタ・アドレス・テーブルを更新し、そして前のＡＰは前の無線ハブからメッセージを受信した後、自分のＭＡＣフィルタ・アドレス・テーブルおよびコネクション・テーブルを更新する。

【０２８３】代わりに、ホーム登録サーバが新しいフォーリン登録サーバからの登録要求を認証し、既存のホームＩＷＦが使えないことを知った後（図３７）、ホーム登録サーバは新しいホームＩＷＦを選定し、現在のＰＰＰサーバ（たとえば、接続されているＩＳＰイントラネットのＰＰＰサーバ）に対する新しいレベル２のトンネル・プロトコル・トンネル（Ｌ２ＴＰトンネル）を作るよう、その新しいホームＩＷＦに指示する。次に、ホーム登録サーバはそのＬ２ＴＰトンネル・トラヒックを新しいホームＩＷＦに対して転送するよう、前のＩＷＦに指示する。

【０２８４】次に、ホーム登録サーバは新しいフォーリン登録サーバに対して新しく割り当てられたサービスしているＩＷＦに対する新しいＩ－ＸＴｕｎｎｅｌを作るよう、新しいホームＩＷＦに指示する。また、ホーム登録サーバは前のフォーリン登録サーバに対して登録解除のメッセージをも送信し、そして前のフォーリン・ネットワークの既存のサービスしているＩＷＦに対する既存のＩ－ＸＴｕｎｎｅｌを破棄するよう、ホームＩＷＦに指示する。肯定のＩ－ＸＴｕｎｎｅｌ作成応答および肯定のＩ－ＸＴｕｎｎｅｌ破棄応答をホームＩＷＦから受信すると、ホーム登録サーバは登録応答を新しいフォーリン登録サーバに対して送信する。

【０２８５】次に、新しいフォーリン登録サーバはその新しい無線ハブに対するＸＴｕｎｎｅｌを作るよう、その新しく割り当てられたＩＷＦに指示する。肯定のＸＴｕｎｎｅｌ作成応答を受信すると、フォーリン登録サーバは登録応答をエンド・システムに対して送信する。登録応答が新しい無線ハブに到着すると、その新しい無線ハブにあるコネクション・テーブルが、新しいＡＰに対するそのコネクションを反映するように更新される。新しいＡＰは新しい無線ハブからメッセージを受信した後、自分のＭＡＣフィルタ・アドレス・テーブルおよびコネクション・テーブルを更新し、登録応答がエンド・システムに対して転送される。

【０２８６】前のフォーリン登録サーバは前の無線ハブに対するＸＴｕｎｎｅｌを破棄するよう、前のＩＷＦに指示する。肯定のＸＴｕｎｎｅｌ破棄応答を受信したとき、あるいはＸＴｕｎｎｅｌの破棄要求と同時に、前のフォーリン登録サーバは前の無線ハブに対して解放メッセージを送信する。その解放メッセージを受信すると、前の無線ハブは自分のコネクション・テーブルおよびＭＡＣフィルタ・アドレス・テーブルを更新し、そして前のＡＰは前の無線ハブからメッセージを受信した後、自分のＭＡＣフィルタ・アドレス・テーブルおよびコネクション・テーブルを更新する。

【０２８７】本発明のシステムに従って構築されたエンド・システムは、提案されているＩＥＴＦモバイルＩＰ標準に従って構築されたネットワークと相互運用可能であり、そして提案されているＩＥＴＦモバイルＩＰ標準に従って構築されたエンド・システムは本発明に従って構築されたネットワークと相互運用可能である。本発明のシステムとＩＥＴＦのモバイルＩＰ（ＲＦＣ　２００２、標準ドキュメント）との間の相違点は次の事項を含む。

【０２８８】（ｉ）本発明のシステムは提案されているＩＥＴＦモバイルＩＰ標準の中のようなフラット構造ではなく、モビリティ管理に対する階層的な概念である。小さい領域内での小さい移動はネットワーク・レベルの登録は行われない。マイクロ・モビリティは新しいＸＴｕｎｎｅｌのセットアップと既存のＸＴｕｎｎｅｌの破棄を伴うグローバル・モビリティは最小限、新しいＩＸＴｕｎｎｅｌのセットアップと既存のＩＸＴｕｎｎｅｌの破棄とを、ＸＴｕｎｎｅｌのセットアップ／破棄とは別に必要とする。また、グローバル・モビリティは新しいＬ２ＴＰトンネルのセットアップおよび、既存のＬ２ＴＰトンネルから新しいＬ２ＴＰトンネルへのＬ２ＴＰのステートの転送を必要とする。

【０２８９】（ii）本発明においては、１つのユーザ名に１つの範囲を加えたものがリモートのダイヤルアップ

・ユーザを識別するために使われ、提案されているＩＥＴＦモバイルＩＰ標準の場合におけるような固定のホーム・アドレスとは異なる。

【０２９０】（iii）本発明においては、登録およびルーティングの機能は別のエンティティによって実行される。この２つの機能は提案されているＩＥＴＦモバイルＩＰ標準においては、ホーム・エージェントによって実行され、そして提案されているＩＥＴＦモバイルＩＰ標準においては両方の機能がフォーリン・エージェントによって実行される。対照的に、本発明の１つの実施形態においては、登録は登録サーバにおいて実行され、そしてルーティングの機能はホームおよびフォーリンのＩＷＦおよび無線ハブ（アクセス・ハブとも呼ばれる）によって実行される。

【０２９１】（ｉｖ）本発明のシステムはＰＰＰセッション当たりに３つのトンネルを利用する。ＸＴｕｎｎｅｌは無線ハブとサービスしているＩＷＦとの間のリンク層のトンネル以上のものである。サービスしているＩＷＦとホームＩＷＦとの間のＩ－ＸＴｕｎｎｅｌは、提案されているＩＥＴＦモバイルＩＰ標準の中のホーム・エージェントとフォーリン・エージェントとの間のトンネルに比較的よく似ている。しかし、それはモバイルＩＰ標準によって提案されているトンネル以上の追加の機能も備えている。Ｌ２ＴＰトンネルはホームＩＷＦがＰＰＰサーバでないときだけ使われる。これらのトンネルの数は以前に説明されたように、いくつかの機能を同じノードの中に組み合わせることによって減らすことができる。

【０２９２】（ｖ）本発明においては、無線登録はＰＰＰセッションが開始される前に発生し、一方、提案されているＩＥＴＦモバイルＩＰ標準においては、ＰＰＰセッションがそのオープン状態に入った後、モバイルＩＰ登録が発生する。

【０２９３】（ｖｉ）本発明においては、エージェントの公示情報を公示するネットワーク・エンティティ（すなわち、無線ハブ）は、エンド・システムに対する直接のリンク上にはなく、一方、提案されているＩＥＴＦモバイルＩＰ標準の場合は、そのエージェントの公示は、そのエンド・システムがフォーリン・エージェントと直接のリンクを有していることを意味する１のＴＴＬを有していなければならない。さらに、本発明のシステムにおけるエージェントの公示は、提案されているＩＥＴＦモバイルＩＰ標準の中でのようなＩＣＭＰルータの公示に対する拡張ではない。

【０２９４】本発明のエンド・システムはエージェントの要請をサポートする必要がある。本発明のシステムにおいてエンド・システムが、提案されているＩＥＴＦモバイルＩＰ標準をサポートしているネットワークを訪問するとき、それはエージェントの公示を聴取するまで待機する。程良いタイム・フレーム内にエージェントの公示を受信しなかった場合、エンド・システムはエージェントの要請をブロードキャストする。

【０２９５】本発明においては、ネットワーク・オペレータが提案されているＩＥＴＦモバイルＩＰ標準をサポートする他のネットワークとネゴシエートし、他のネットワークの使用を希望している本発明のエンド・システムに対してホーム・アドレスを割り当てることができるようにすることができる。エージェントの公示を受信すると、本発明のシステムのエンド・システムは自分が訪問しているネットワークが本発明に従っているネットワークではなく、したがって、登録するためにはその割り当てられたホーム・アドレスを使うことを知ることができる。

【０２９６】提案されているＩＥＴＦモバイルＩＰ標準をサポートしているネットワークの場合、ＰＰＰセッションはモバイルＩＰの登録の前に開始され、ＰＰＰサーバはそのようなネットワークにおいてはフォーリン・エージェントと同じ場所にあると仮定される。１つの実施形態においては、ＳＮＡＰヘッダが本発明のシステムのＭＡＣフレームの中にＰＰＰフレームをカプセル化するために使われ（イーサネットのフォーマットと同様な方法で）、フォーリン・エージェントがこのフォーマットをイーサネットのカプセル化についての私有のＰＰＰフォーマットとして解釈する。したがって、本発明のシステムのエンド・システムおよびそのＰＰＰピアはフォーリン・エージェントがエージェントの公示を送信し始める前にオープン状態に入ることができ、そして本発明のシステムのエンド・システムは登録することができる。

【０２９７】提案されているＩＥＴＦモバイルＩＰ標準をサポートしているエンド・システムが本発明のタイプのネットワークの中で正常に動作できるようにするために、そのようなモバイルは少なくともＭＡＣ層の登録と同様なことを実行できる。エージェントの公示メッセージのフォーマットを、提案されているモバイルＩＰ標準のエージェントの公示メッセージのフォーマットと同様なものにすることによって、訪問しているエンド・システムはそのエージェントの公示を解釈し、無線ハブに登録することができる。本発明においては、登録要求および応答のメッセージは提案されているＩＥＴＦモバイルＩＰ標準の登録要求および応答のメッセージと似ており（不必要な拡張なしで）、本発明のシステムのモビリティ管理の特徴の他の部分は、訪問しているエンド・システムにとってはトランスペアレントであるようになっている。

【０２９８】提案されているＩＥＴＦモバイルＩＰ標準をサポートしているエンド・システムは、ＰＰＰセッションがモバイルＩＰの登録の前に開始されることを期待しているので、本発明のシステムの無線ハブにおけるオプションの機能はＭＡＣ層の登録の後、ＰＰＰのＬＣＰ、ＮＣＰパケットを解釈し始める。

【０２９９】ハンドオフの間にトラヒックが消失するのを避けるために、本発明のシステムのモビリティ管理はメイク・ビフォー・ブレイクの概念に基づいている。ローカル・モビリティの場合、メイク・ビフォー・ブレイクのコネクションは新しいＡＰによって無線ハブに対して中継されるＭＡＣ層の登録メッセージをブロードキャスト・メッセージにすることによって達成される。その方法で、前のＡＰは新しい登録について聴取することができ、その新しいＡＰに対して転送されていないエンド・システムに向けられているパケットを転送することができる。

【０３００】マイクロ・モビリティの場合、新しい無線ハブに関する情報はサービスしているＩＷＦと前のＷＨとの間で交換されるＸＴｕｎｎｅｌ破棄のメッセージの中に含まれている。そのようにして、前の無線ハブはサービスしているＩＷＦからＸＴｕｎｎｅｌ破棄メッセージを聴取したときに、新しい無線ハブに対してバッファされているパケットを転送することができる。代わりに、ＩＷＦにあるＲＬＰ層はそれまでに前の無線ハブによってアクノレッジされていたシーケンス番号を知る。

【０３０１】同時に、ＩＷＦは前の無線ハブに対して送信された最新のパケットの現在の送信シーケンス番号を知る。したがって、ＩＷＦは新しい方のパケットを新しい方の無線ハブに対して送信する前に、その新しい無線ハブに対してこれらの２つの番号の間に順序付けられているパケットを転送することができる。ＲＬＰ層は重複しているパケットをフィルタすることができると仮定されている。第２の方法は、前の無線ハブが互いに直接通信することができない可能性があるために、第１の方法よりもおそらく好ましい。

【０３０２】マクロ・モビリティの場合、前のサービスしているＩＷＦは前の無線ハブから新しい無線ハブに対して行われるパケット転送に加えて、新しいサービスしているＩＷＦに対してパケットを転送することができる。行う必要があるのは、ＩＸＴｕｎｎｅｌの破棄メッセージの中で新しいサービスしているＩＷＦに対して新しいサービスしているＩＷＦのアイデンティティを転送することだけである。同じ結果を達成するための別の方法は、その仕事を前のサービスしているＩＷＦに頼むのではなく、新しいサービスしているＩＷＦに対して欠落しているパケットをホームＩＷＦが転送するようにさせる方法である。というのは、ホームＩＷＦは前のサービスしているＩＷＦによって最近アクノレッジされたＩＸＴｕｎｎｅｌのシーケンス番号およびホームＩＷＦによって送信された現在のＩＸＴｕｎｎｅｌのシーケンス番号を知っているからである。

【０３０３】ハンドオフの間でのトラヒックの消失を最小化することができるように、１つのモバイル、ＡＰ、無線ハブ、ＩＷＦ当たりにどの程度多くのバッファが割り当てられるべきかを推定する方法は、ＡＰ、無線ハブ、ＩＷＦに対するパケットの到着レートおよびハンドオフ時間をそのエンド・システムに推定させる方法である。この情報がＩＷＦの無線ハブの前のＡＰに対して渡され、ハンドオフ時にそのＩＷＦの無線ハブの新しいＡＰに対してそれぞれどれだけ多くのトラヒックが転送されるはずであるかを知る。

【０３０４】本発明においてルートの最適化を実現するために、エンド・システムはサービスしているＩＷＦに最も近いＰＰＰサーバを選定する。ルートを最適化しない場合、転送の遅延時間および物理的な回線の使用が過剰になる可能性がある。

【０３０５】たとえば、ニューヨーク市にあるホーム・ネットワークに加入しているエンド・システムが香港へロームすることができる。香港のＩＳＰに対するリンクを設立するために、エンド・システムは香港にある無線ハブの中でサービスしているＩＷＦを設立し、そしてニューヨーク市にあるホーム・ネットワークの中でホームＩＷＦを設立していることになる。その時、メッセージがエンド・システムから回送され（香港へロームされ）、サービスしているＩＷＦ（香港にある）を通って、またホームＩＷＦ（ニューヨーク市にある）を通って香港のＩＳＰへ戻される。

【０３０６】好ましい方法はサービスしているＩＷＦ（香港にある）から香港のＩＳＰに直接に接続することである。サービスしているＩＷＦはホームＩＷＦと同様に働く。この実施形態においては、ローミングの契約がホームとフォーリンの無線プロバイダの間に存在する。さらに、各種のアカウンティング／料金請求システムが互いに自動的に通信し、料金請求の情報が共有されるようにする。アカウンティングおよび料金請求の情報の交換は、ＩＥＴＦのＲＯＡＭＯＰＳワーキング・グループによって提案されている標準などの標準を使って実装することができる。

【０３０７】しかし、サービスしているＩＷＦは依然として最も近いＰＰＰサーバ（たとえば、香港のＩＳＰ）を発見しなければならない。この実施形態においては、フォーリン登録サーバはエンド・システムからの登録要求を受信したとき、ＰＰＰサーバ（たとえば、香港のＩＳＰ）にエンド・システムが接続を望んでいることを知る。フォーリン登録サーバは、サービスしているＩＷＦがホームＩＷＦよりその望まれているＰＰＰサーバ（たとえば、香港のＩＳＰ）により近いことを知ると、フォーリン登録サーバはサービスしているＩＷＦに対して、その最も近いＰＰＰサーバ（ホーム登録サーバに対して最も近いＰＰＰサーバおよびホームＩＷＦとは対照的に）Ｌ２ＴＰトンネルを設立するよう指示する。次に、フォーリン登録サーバはそのエンド・システムがサービスしているＩＷＦおよびフォーリンＰＰＰによってサービスされていることをホーム登録サーバに通知する。

【０３０８】他の実施形態においては、フォーリン登録

75

サーバは、エンド・システムからの登録要求を受信したとき、サービスしているＩＷＦがホームＩＷＦより望まれているＰＰＰサーバ（たとえば、香港のＩＳＰ）により近いことを知る。フォーリン登録サーバはサービスしているＩＷＦの情報およびルートの最適化が好ましいことの通知を示している付加されたメッセージを付けて登録要求メッセージをホーム登録サーバに対して中継する。同時に、フォーリン登録サーバはＰＰＰサーバに対してＬ２ＴＰトンネルを設立するようサービスしているＩＷＦに指示する。登録要求を承認すると、ホーム登録サーバはＬ２ＴＰの状態をフォーリンＩＷＦに対して転送するよう、ホームＩＷＦに指示する。

【０３０９】無線エンド・ユーザがロームすることができる新しいネットワーク・アーキテクチャの好適な実施形態（それは、例を示すことを意図していて、限定するものではない）で説明してきたが、この分野の技術に熟達した人であれば、上記の内容に従って変更および変形版を作ることができることを留意されたい。たとえば、ここで説明されたコネクション・リンクは既知のコネクション・プロトコル（たとえば、ＩＰ、ＴＣＰ／ＩＰ、Ｌ２ＴＰ、ＩＥＥＥ８０２．３など）に対する参照を行うことができる。しかし、そのシステムはコネクション・リンクにおいて、同じか、あるいは類似のデータ配送機能を提供する他のコネクション・プロトコルを考慮する。上記の実施形態において動作しているエージェントはソフトウェア制御型のプロセッサの形式、あるいは他の形式の制御（たとえば、プログラマブル・ロジック・アレイなど）であってもよい。動作しているエージェントは上記のようにグループ化されるか、あるいはここで説明されているコネクションの内容を保ちながら、そしてここで説明されたセキュリティおよび認証の内容を前提として、別の形式でグループ化することができる。さらに、単独のアクセス・ポイント、アクセス・ハブ（すなわち、無線ハブ）またはインターワーキング機能（ＩＷＦユニット）はマルチチャネル機能を提供することもできる。したがって、単独のアクセス・ポイントまたはアクセス・ハブまたはＩＷＦユニットは複数のエンド・システムからのトラヒックについて動作することができ、そして別々のアクセス・ポイント、アクセス・ハブまたはＩＷＦユニットとしてここで記述されている事項は、単独のマルチチャネル・アクセス・ポイント、アクセス・ハブまたはＩＷＦユニットについても等しく考慮される。したがって、添付の特許請求の範囲に記載した本発明の精神および範囲を逸脱することなしに、開示されたシステムの特定の実施形態における変更がなされ得ることを理解されたい。

【０３１０】このシステムを詳細に、そして特許法によって特に必要とされるように説明してきたが、開封特許状によって請求され、そして保護されることが望ましい事項が添付の特許請求の範囲に説明されている。

76

【図面の簡単な説明】

【図１】公衆交換電話網を通じての既知のリモート・アクセス・アーキテクチャの構成図である。

【図２】本発明による無線パケット交換データ網を通じてのリモート・アクセス・アーキテクチャの構成図である。

【図３】ローミングのシナリオを示している図２のネットワークのアーキテクチャの選択された部分の構成図である。

【図４】ローカルのアクセス・ポイントを備えている基地局の構成図である。

【図５】リモートのアクセス・ポイントを備えている基地局の構成図である。

【図６】リモートのアクセス・ポイントを備えた基地局の構成図であり、リモートのアクセス・ポイントのいくつかは無線幹線コネクションを使って接続されている。

【図７】ローカルのアクセス・ポイントに対するプロトコル・スタックの図である。

【図８】無線幹線を備えたリモートのアクセス・ポイントに対するプロトコル・スタックの図である。

【図９】無線幹線を備えたリモートのアクセス・ポイントをサポートするための、基地局における中継機能に対するプロトコル・スタックの図である。

【図１０】図９に示されている中継機能を実装するためのプロトコル・スタックの図である。

【図１１】ローカルのアクセス・ポイントをサポートするための基地局の中継機能に対するプロトコル・スタックの図である。

【図１２】図２のネットワークのアーキテクチャの選択された部分の構成図であり、ホーム・ネットワークからホーム・ネットワークに登録している第１のエンド・システムおよび、ホーム・インターワーキング機能をアンカーとして使ってフォーリン・ネットワークからホーム・ネットワークに登録している第２のシステムを示す。

【図１３】図２のネットワークのアーキテクチャの選択された部分の構成図であり、ホーム・ネットワークからホーム・ネットワークに登録している第１のエンド・システムおよび、サービスしているインターワーキング機能をアンカーとして使ってフォーリン・ネットワークからホーム・ネットワークに登録している第２のシステムを示す。

【図１４】フォーリン・ネットワークからホーム・ネットワークに登録するため、そしてデータ・リンクを設立し、認証し、構成するための要求メッセージと応答メッセージのラダー・ダイアグラムである。

【図１５】図２のネットワークのアーキテクチャの選択された部分の構成図であり、ホーム・ネットワークの中のモバイルをホーム・ネットワークから登録するための登録要求および応答を示す。

【図１６】図２のネットワークのアーキテクチャの選択

された部分の構成図であり、ホーム・ネットワークの中のモバイルをフォーリン・ネットワークから登録するための登録要求および応答を示す。

【図１７】セル・サイトがローカルのアクセス・ポイントを備えている場合の、ホーム・ネットワークの中のエンド・システムとホーム・ネットワークの中のインターワーキング機能との間の通信を示しているプロトコル・スタックの構成図である。

【図１８】セル・サイトが無線幹線を通じて無線ハブに結合されているリモートのアクセス・ポイントを備えている場合の、ホーム・ネットワークの中のエンド・システムとホーム・ネットワークの中のインターワーキング機能との間の通信を示しているプロトコル・スタックの構成図である。

【図１９】ローム（移動）しているエンド・システムに対して結合されている基地局と、ホーム・インターワーキング機能との間の通信を示しているプロトコル・スタックの構成図である。

【図２０】ホーム・ネットワークの中のインターワーキング機能を通じてのインターネット・サービス・プロバイダに対するホーム・ネットワークの中のエンド・システムとの間の通信を示しているプロトコル・スタックの構成図である。

【図２１】フォーリン・ネットワークの中のエンド・システムとホーム・ネットワークの中のホーム登録サーバとの間での、登録フェーズにおける通信を示しているプロトコル・スタックの構成図である。

【図２２】アカウンティング・データを処理して顧客の料金請求システムに対して渡す流れを示している処理の流れ図である。

【図２３】ホーム・ネットワークの中、およびフォーリン・ネットワークの中のエンド・システムに対する登録プロセスをそれぞれ示しているラダー・ダイアグラムである。

【図２４】ホーム・ネットワークの中、およびフォーリン・ネットワークの中のエンド・システムに対する登録プロセスをそれぞれ示しているラダー・ダイアグラムである。

【図２５】ＰＰＰプロトコルがホーム・ネットワークのインターワーキング機能においてターミネートする場合、およびＰＰＰプロトコルがＩＳＰまたはイントラネットにおいてターミネートする場合の、ホーム・ネットワークにおけるエンド・システムのコネクションをそれぞれ示しているプロトコル・スタックの図である。

【図２６】ＰＰＰプロトコルがホーム・ネットワークのインターワーキング機能においてターミネートする場合、およびＰＰＰプロトコルがＩＳＰまたはイントラネットにおいてターミネートする場合の、ホーム・ネットワークにおけるエンド・システムのコネクションをそれぞれ示しているプロトコル・スタックの図である。

【図２７】ＰＰＰプロトコルがフォーリン・ネットワークのインターワーキング機能においてターミネートする場合、およびＰＰＰプロトコルがＩＳＰまたはイントラネットにおいてターミネートする場合の、フォーリン・ネットワークにおけるエンド・システムのコネクションをそれぞれ示しているプロトコル・スタックの図である。

【図２８】ＰＰＰプロトコルがフォーリン・ネットワークのインターワーキング機能においてターミネートする場合、およびＰＰＰプロトコルがＩＳＰまたはイントラネットにおいてターミネートする場合の、フォーリン・ネットワークにおけるエンド・システムのコネクションをそれぞれ示しているプロトコル・スタックの図である。

【図２９】ＰＰＰプロトコルがイーサネット・フレームにカプセル化されている場合の、イーサネット経由で無線モデムに対して接続されているエンド・システムを示す。

【図３０】イーサネット・フレームのフォーマットを示す。

【図３１】ＸＷＤヘッダのフィールドを示す。

【図３２】ＰＰＰプロトコルが無線ルータにおいてターミネートする場合の、ローカル・エリア・ネットワークを経由して無線ルータに接続されているエンド・システムを示す。

【図３３】ローカル・ハンドオフのシナリオ、マイクロ・ハンドオフのシナリオ、およびマクロ・ハンドオフのシナリオをそれぞれ示しているラダー・ダイアグラムである。

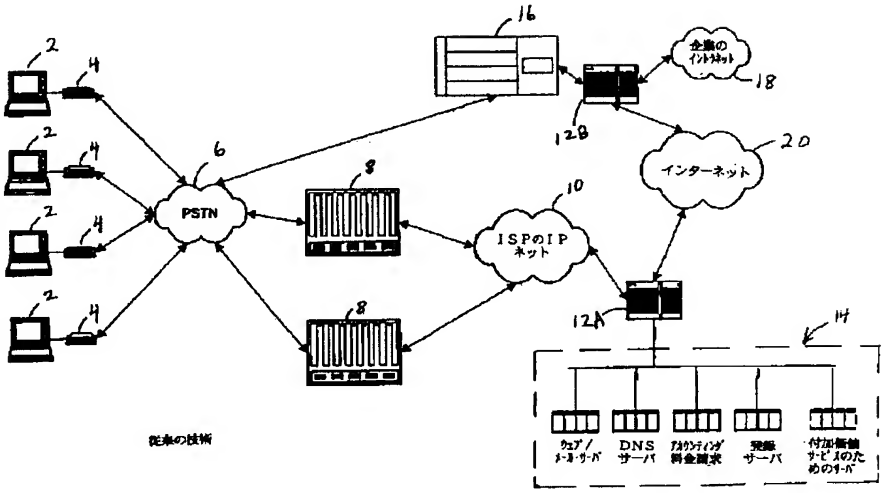
【図３４】ローカル・ハンドオフのシナリオ、マイクロ・ハンドオフのシナリオ、およびマクロ・ハンドオフのシナリオをそれぞれ示しているラダー・ダイアグラムである。

【図３５】ローカル・ハンドオフのシナリオ、マイクロ・ハンドオフのシナリオ、およびマクロ・ハンドオフのシナリオをそれぞれ示しているラダー・ダイアグラムである。

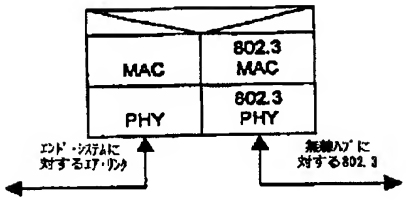
【図３６】フォーリン登録サーバが変化する場合、そしてホーム・インターワーキング機能が変化しない場合の、グローバル・ハンドオフのシナリオを示しているラダー・ダイアグラムである。

【図３７】フォーリン登録サーバおよびホーム・インターワーキング機能の両方が変化する場合の、グローバル・ハンドオフのシナリオを示しているラダー・ダイアグラムである。

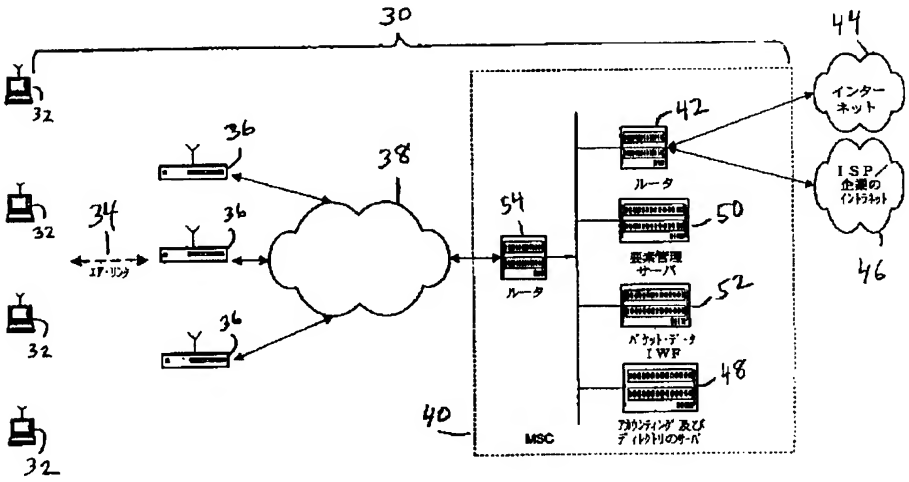
【図１】


PSTN
ISPのIP
ネット
インターネット
企業の
イントラネット
DNS
サーバ
従来の技術

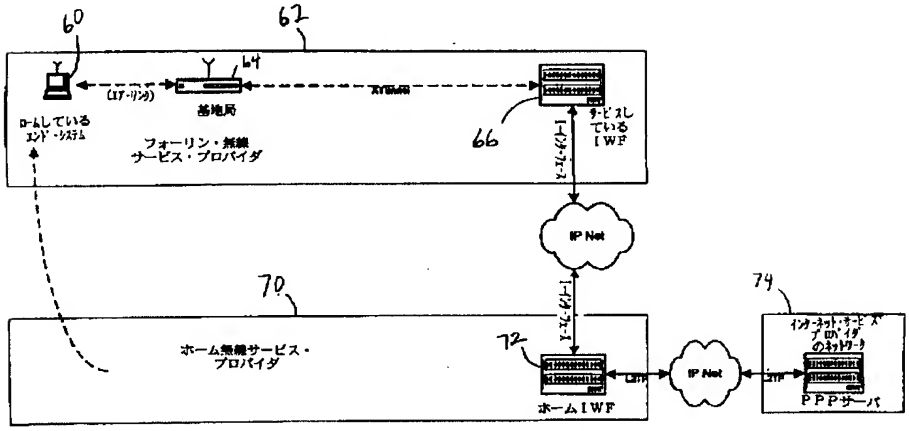
【図７】


MAC
802.3
MAC
PHY
802.3
PHY
エンド・システムに
対するエア・リンク
無線ハブに
対する802.3

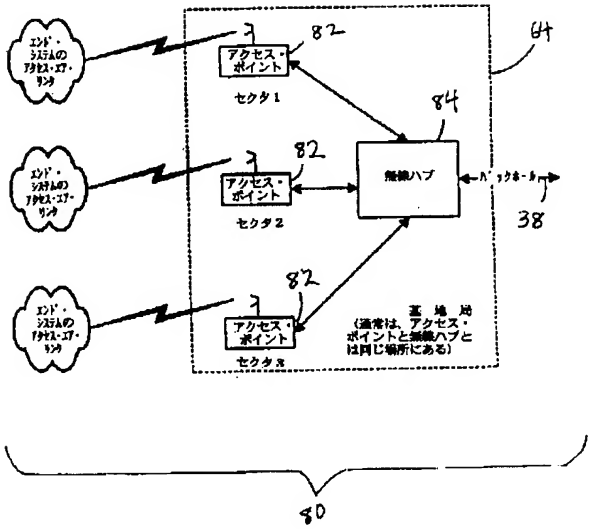
【図２】


インター
ネット
ISP
企業の
イントラネット
ルータ
ルータ
MSC
エア・リンク

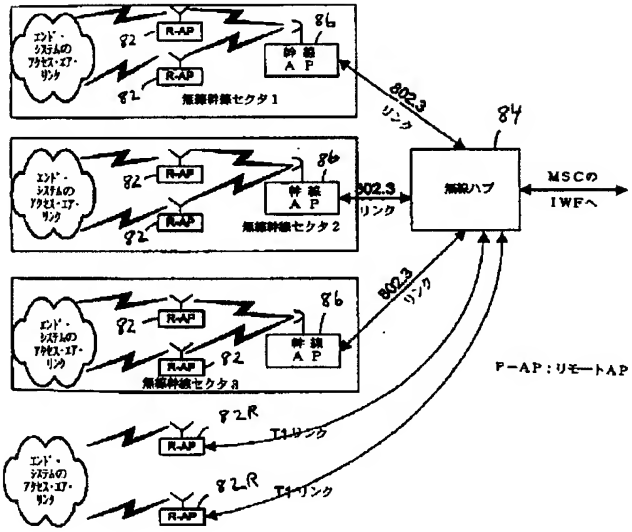
【図３】


基地局
フォーリン・無線
サービス・プロバイダ
サービスしている
IWF
IP Net
ホーム無線サービス・
プロバイダ
ホームIWF
IP Net
PPPサーバ

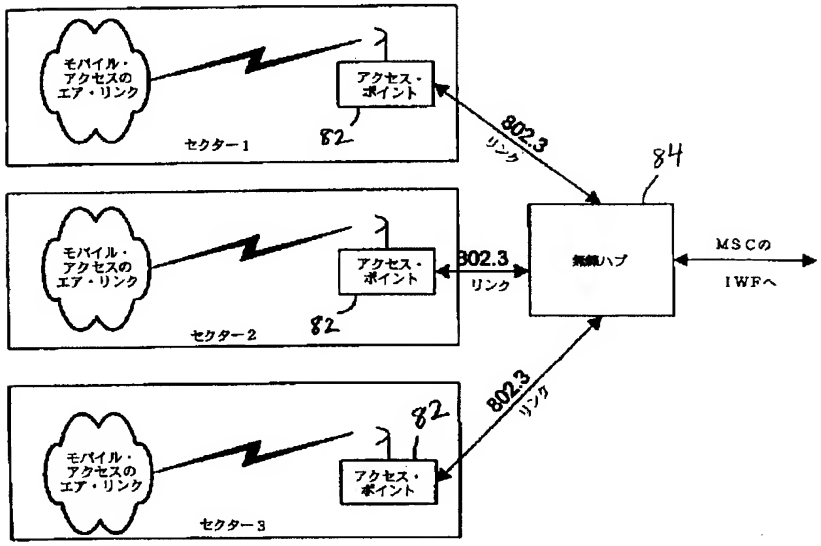
【図４】


エンド・システムのアクセス・エア・リンク
アクセス・ポイント
82
セクタ１
84
無線ハブ
64
セクタ２
38
セクタ３
基地局
(通常は、アクセス・ポイントと無線ハブとは同じ場所にある)
80

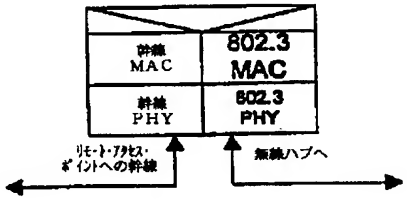
【図６】


R-AP
82
86
幹線AP
無線幹線セクタ１
802.3リンク
84
無線ハブ
MSCのIWFへ
無線幹線セクタ２
無線幹線セクタ３
P-AP：リモートAP
82R
I+リンク

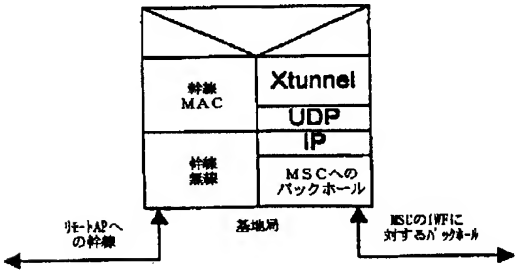
【図５】


モバイル・アクセスのエア・リンク
アクセス・ポイント
82
セクター１
802.3リンク
84
セクター２
無線ハブ
MSCのIWFへ
セクター３

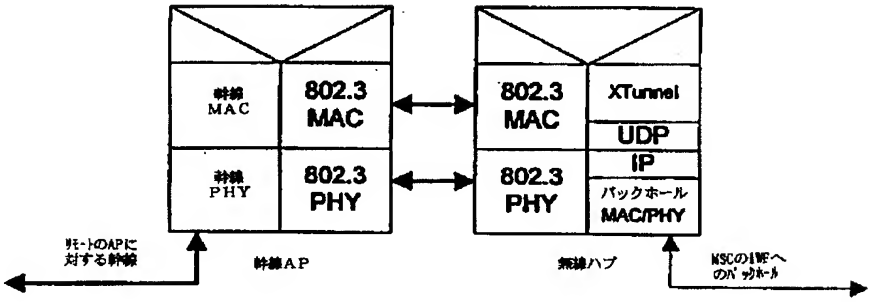
【図８】


幹線MAC
802.3 MAC
幹線PHY
802.3 PHY
リモート・アクセス・ポイントへの幹線
無線ハブへ

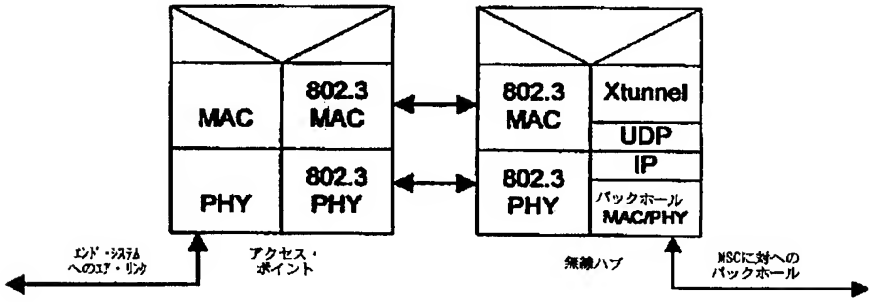
【図９】


幹線MAC
Xtunnel
UDP
IP
幹線無線
MSCへのバックホール
リモートAPへの幹線
基地局
MSCのIWFに対するバックホール

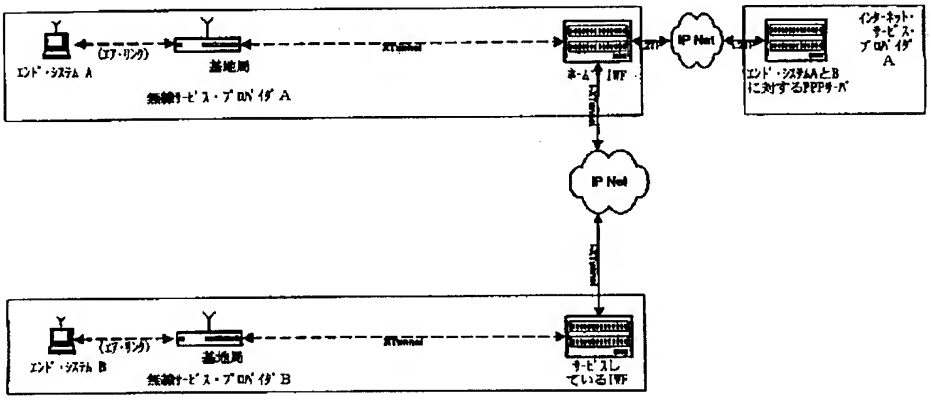
【図１０】



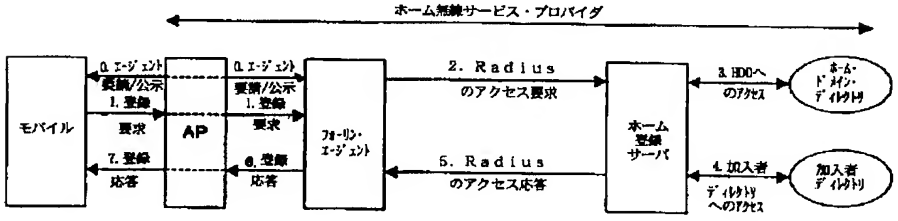
【図１１】



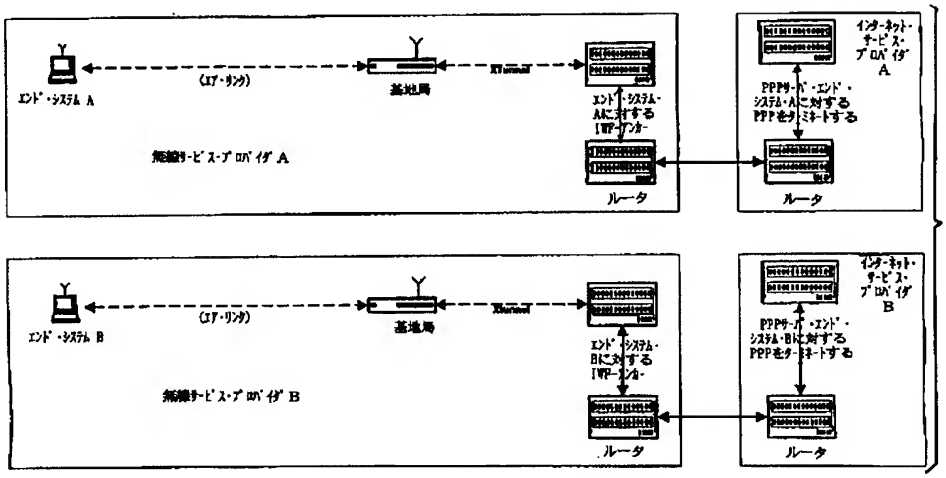
【図１２】



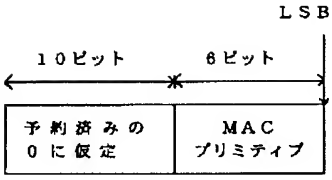
【図１５】



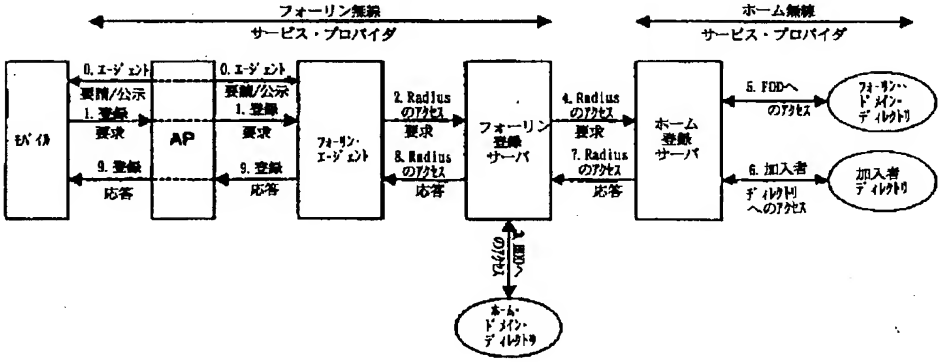
【図１３】



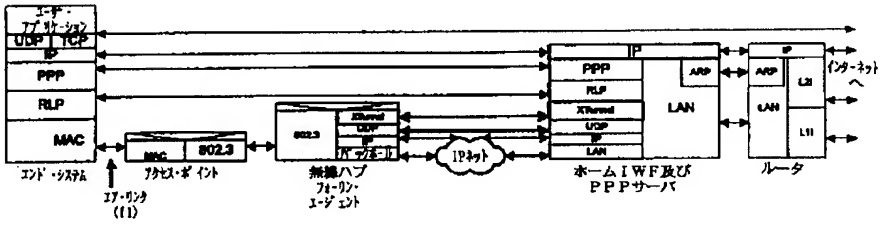
【図３１】



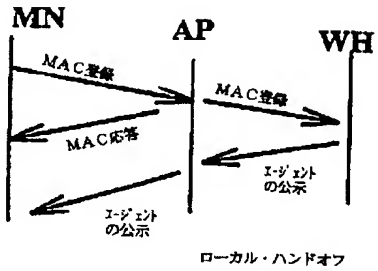
【図１６】



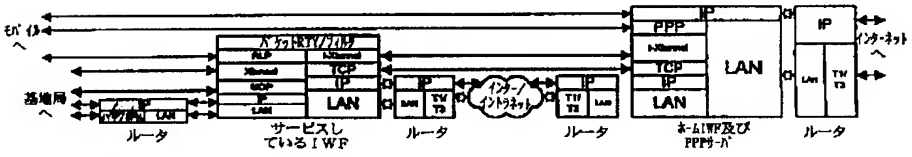
【図１７】



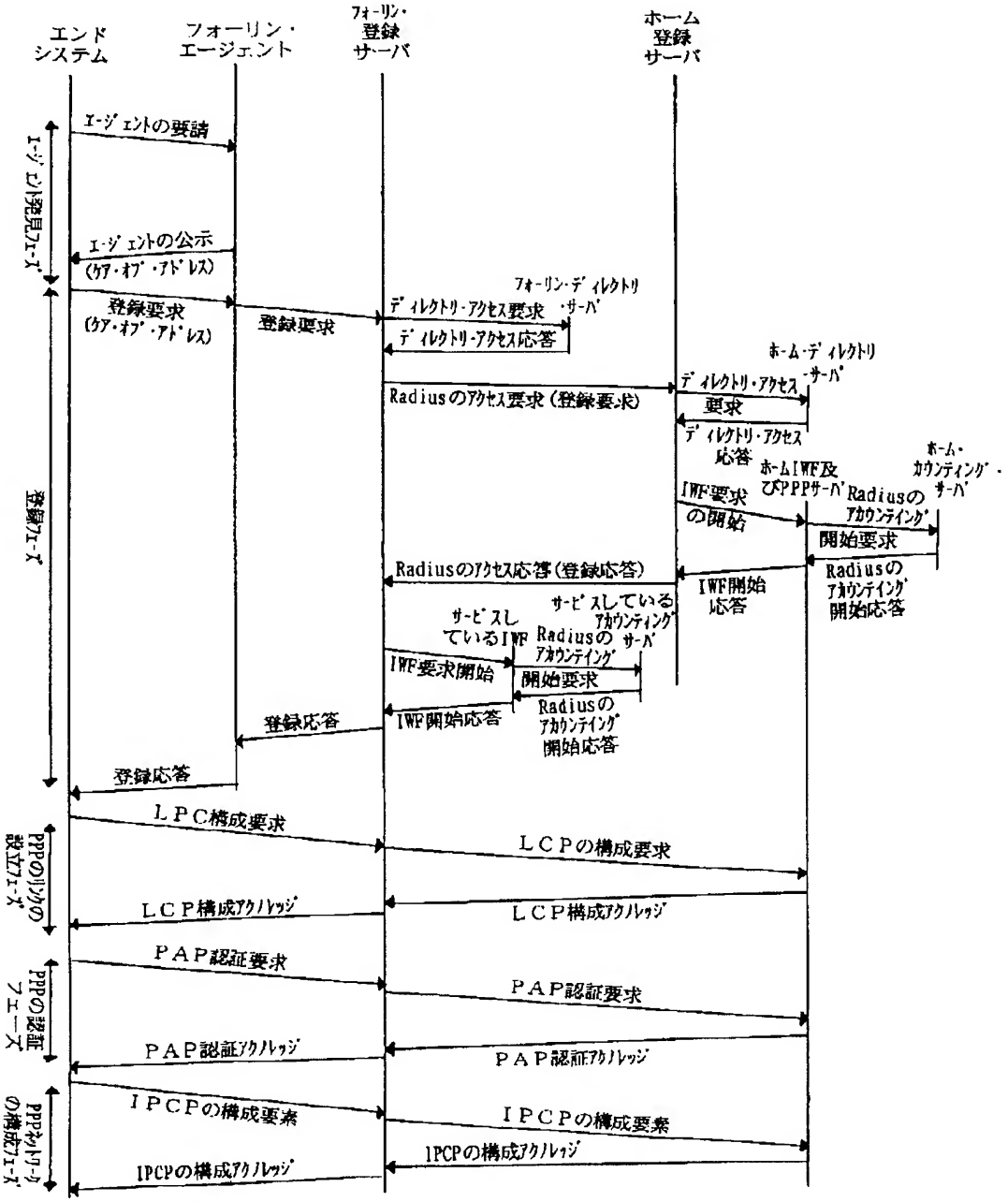
【図３３】



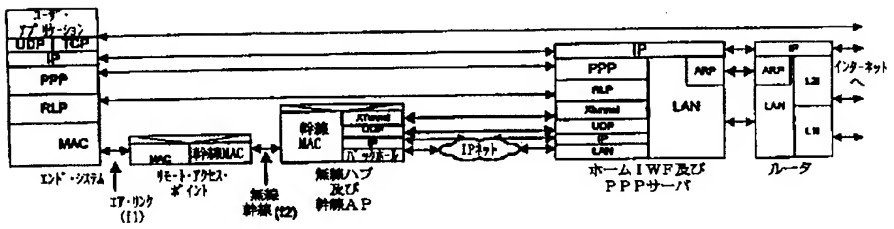
【図１９】



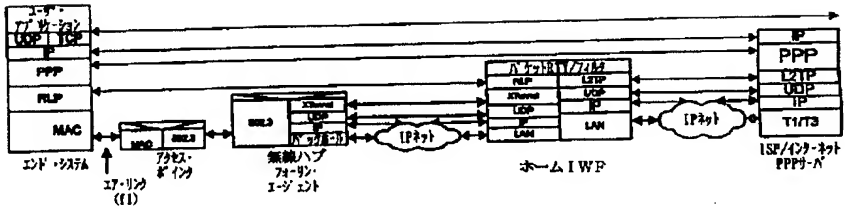
【図１４】


エンド システム
フォーリン・ エージェント
フォーリン・ 登録 サーバ
ホーム 登録 サーバ
エージェント発見フェーズ
エージェントの要請
エージェントの公示
(ケア・オブ・アドレス)
登録フェーズ
登録要求 (ケア・オブ・アドレス)
登録要求
フォーリン・ディレクトリ・サーバ
ディレクトリ・アクセス要求
ディレクトリ・アクセス応答
ホーム・ディレクトリ・サーバ
Radiusのアクセス要求(登録要求)
ディレクトリ・アクセス要求
ディレクトリ・アクセス応答
ホームIWF及びPPPサーバ
IWF要求の開始
Radiusのアカウンティング開始要求
ホーム・カウンティング・サーバ
Radiusのアクセス応答(登録応答)
IWF開始応答
Radiusのアカウンティング開始応答
サービスしているIWF
サービスしているRadiusのアカウンティング・サーバ
IWF要求開始
開始要求
IWF開始応答
Radiusのアカウンティング開始応答
登録応答
登録応答
PPPのリンクの設立フェーズ
ＬＰＣ構成要求
ＬＣＰの構成要求
ＬＣＰ構成アクノレッジ
ＬＣＰ構成アクノレッジ
PPPの認証フェーズ
ＰＡＰ認証要求
ＰＡＰ認証要求
ＰＡＰ認証アクノレッジ
ＰＡＰ認証アクノレッジ
PPPネットワークの構成フェーズ
ＩＰＣＰの構成要素
ＩＰＣＰの構成要素
IPCPの構成アクノレッジ
IPCPの構成アクノレッジ

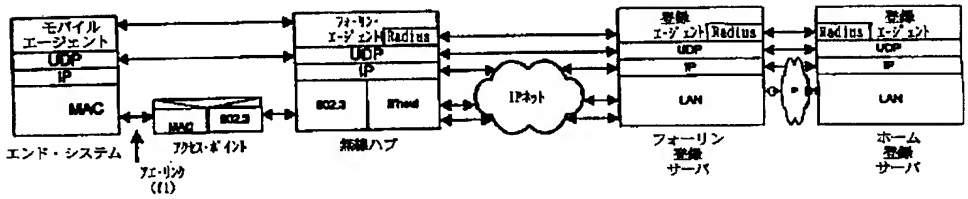
【図１８】


UDP
TCP
IP
PPP
RLP
MAC
エンド・システム
エア・リンク (I1)
リモート・アクセス・ポイント
無線 (I2)
無線ハブ及び無線AP
IPネット
ホームIWF及びPPPサーバ
LAN
ルータ
インターネットへ

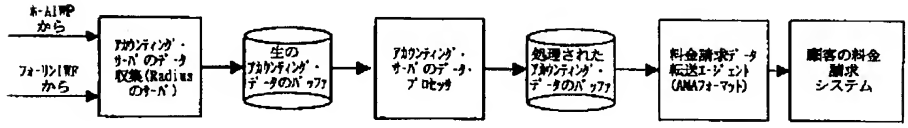
【図２０】



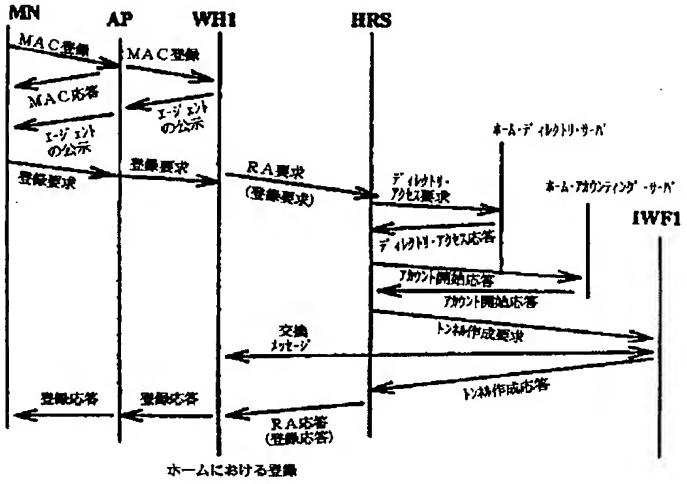
【図２１】



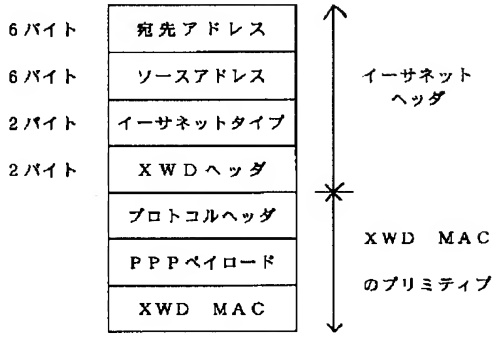
【図２２】



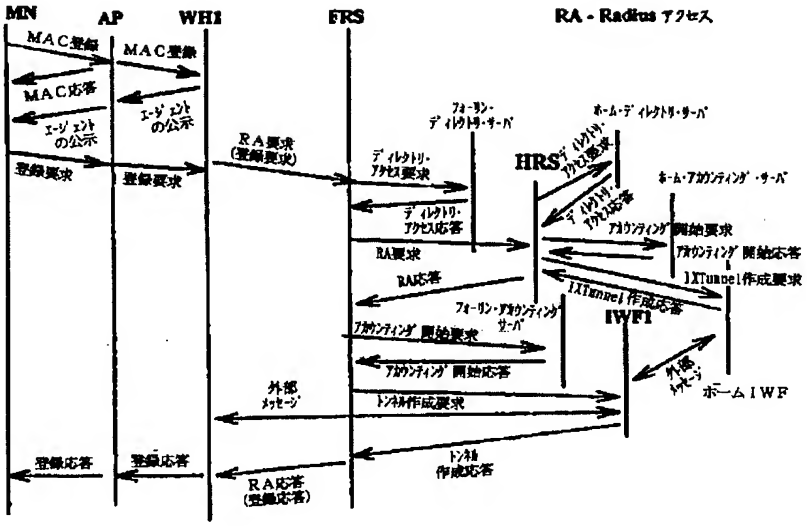
【図２３】



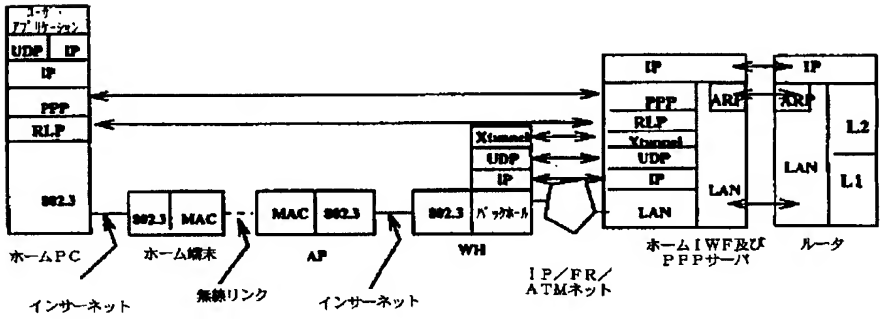
【図３０】



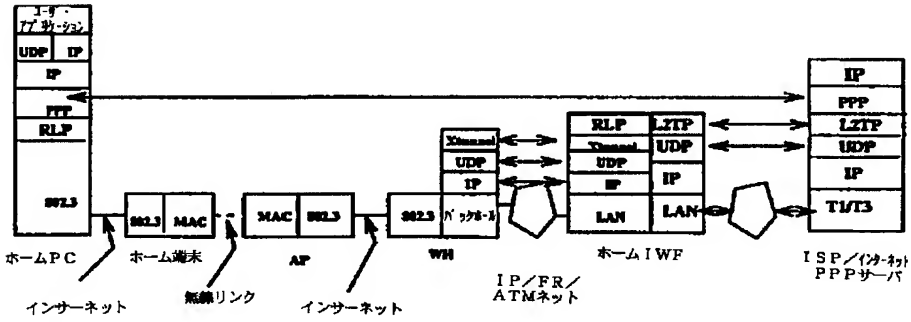
【図２４】


MN
AP
WHI
FRS
RA - Radius アクセス
MAC登録
MAC応答
エージェントの公示
登録要求
RA要求
(登録要求)
ディレクトリ・アクセス要求
ディレクトリ・アクセス応答
HRS
RA要求
RA応答
アカウンティング開始要求
アカウンティング開始応答
IXTunnel作成要求
IXTunnel作成応答
IWF1
ホームIWF
外部メッセージ
トンネル作成要求
トンネル作成応答
登録応答
RA応答
(登録応答)

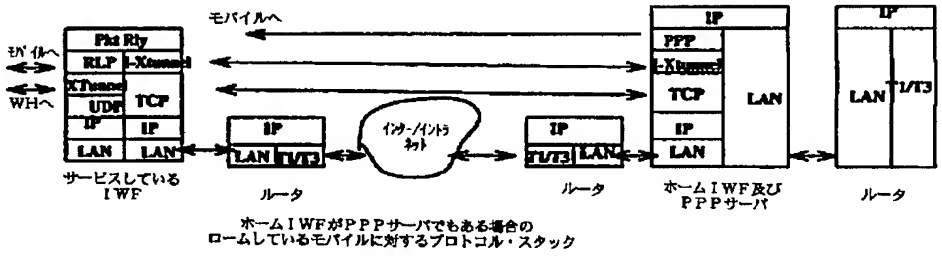
【図２５】


UDP
IP
PPP
RLP
802.3
MAC
Xtunnel
ARP
LAN
L2
L1
ホームPC
ホーム端末
AP
WH
ホームIWF及び
PPPサーバ
ルータ
インターネット
無線リンク
IP／FR／
ATMネット

【図２６】

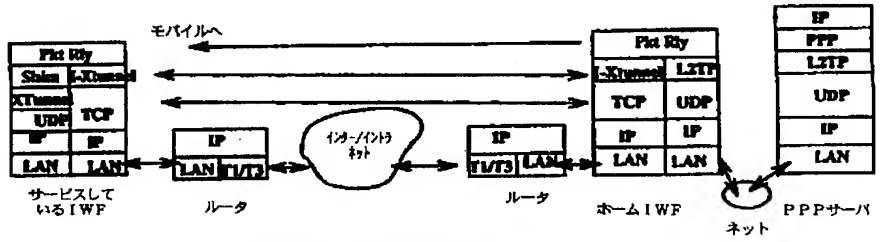

UDP
IP
PPP
RLP
LZTP
802.3
MAC
Xtunnel
T1/T3
ホームPC
ホーム端末
AP
WH
ホームIWF
ISP／インターネット
PPPサーバ
インターネット
無線リンク
IP／FR／
ATMネット

【図２７】



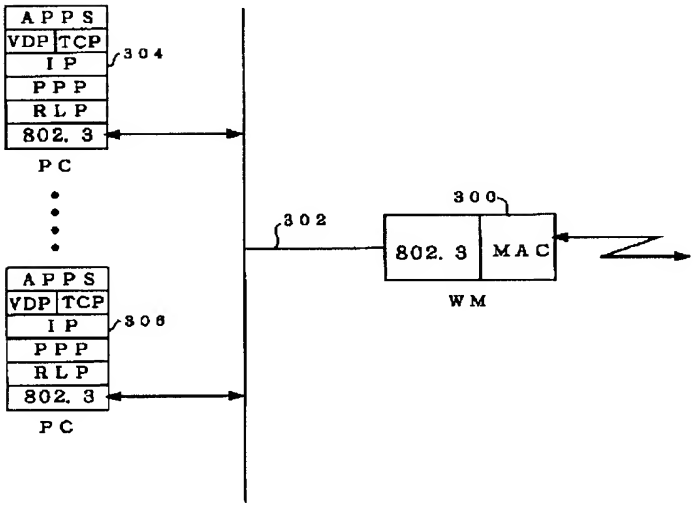
ホームＩＷＦがＰＰＰサーバでもある場合の
ロームしているモバイルに対するプロトコル・スタック

【図２８】

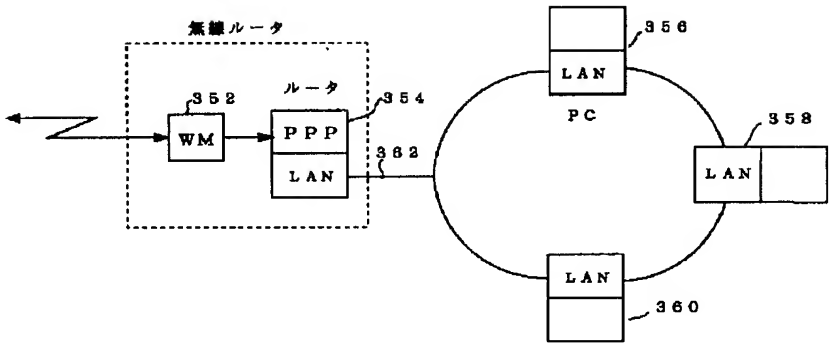


ホームＩＷＦとＰＰＰサーバが分かれている場合の
ロームしているモバイルに対するプロトコル・スタック

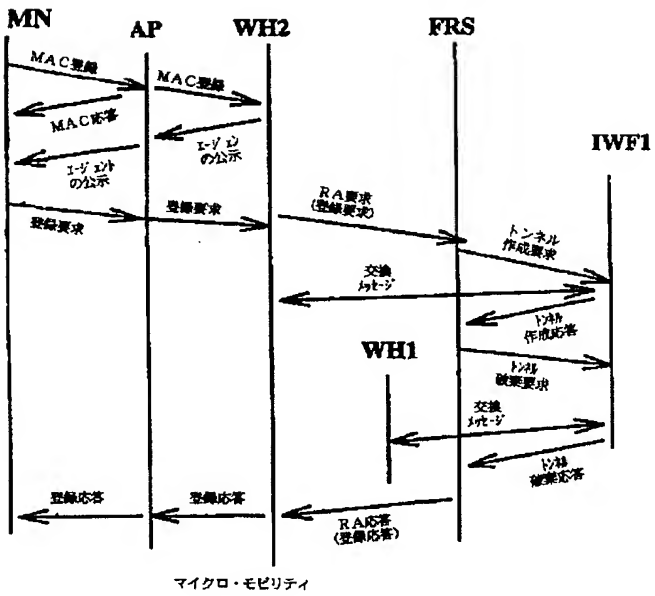
【図２９】



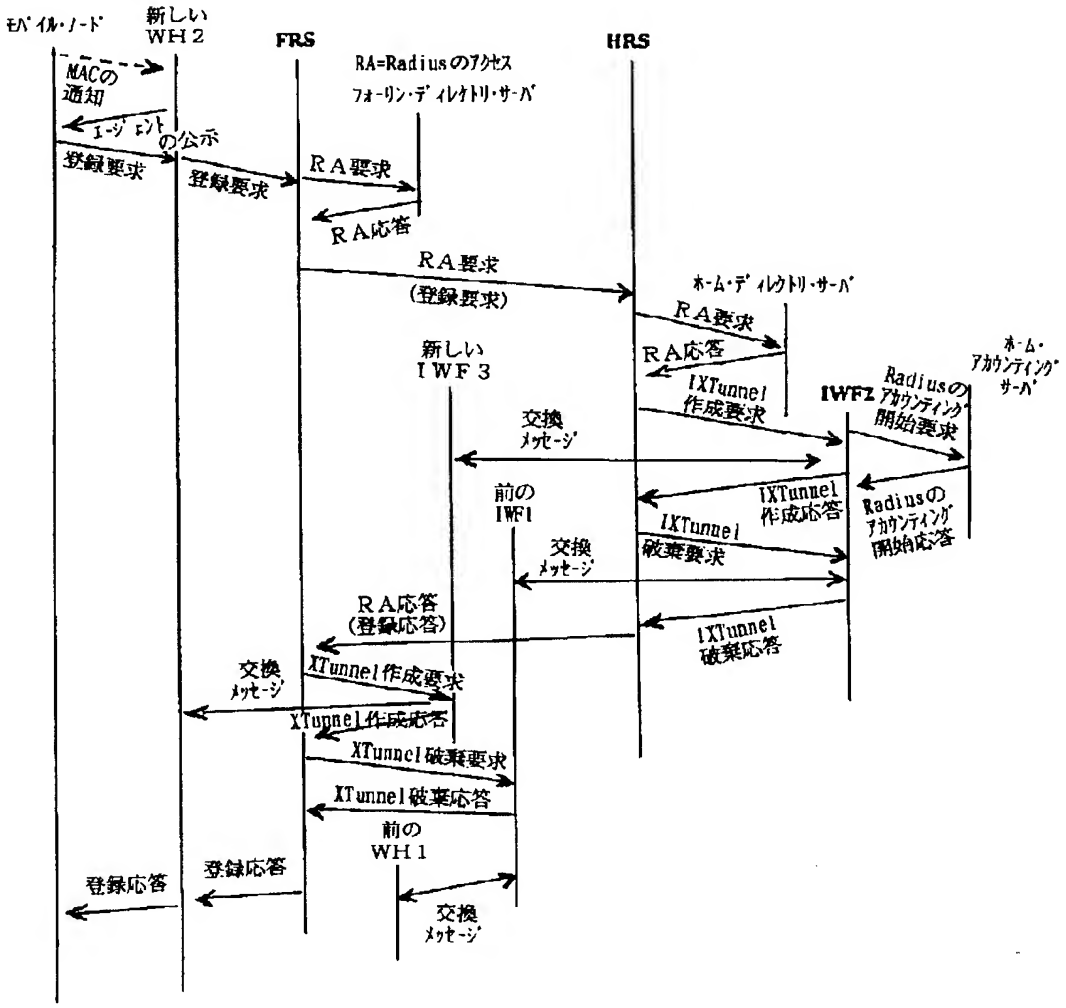
【図３２】


無線ルータ
352
ルータ
354
WM
PPP
LAN
362
356
LAN
PC
358
LAN
LAN
360

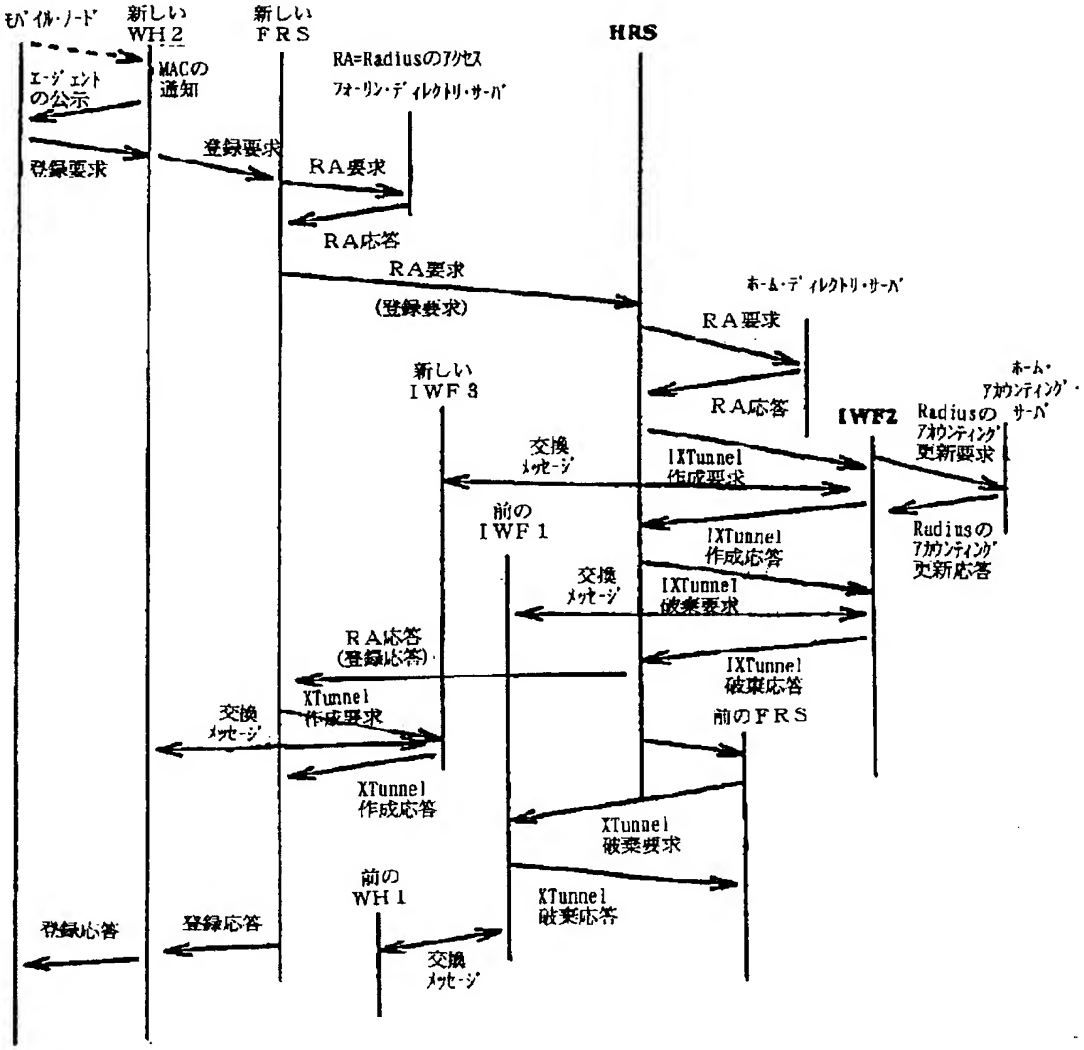
【図３４】


MN
AP
WH2
FRS
IWF1
WH1
MAC登録
MAC応答
エージェントの公示
登録要求
RA要求
(登録要求)
トンネル作成要求
交換メッセージ
トンネル作成応答
トンネル破棄要求
交換メッセージ
トンネル破棄応答
登録応答
RA応答
(登録応答)
マイクロ・モビリティ

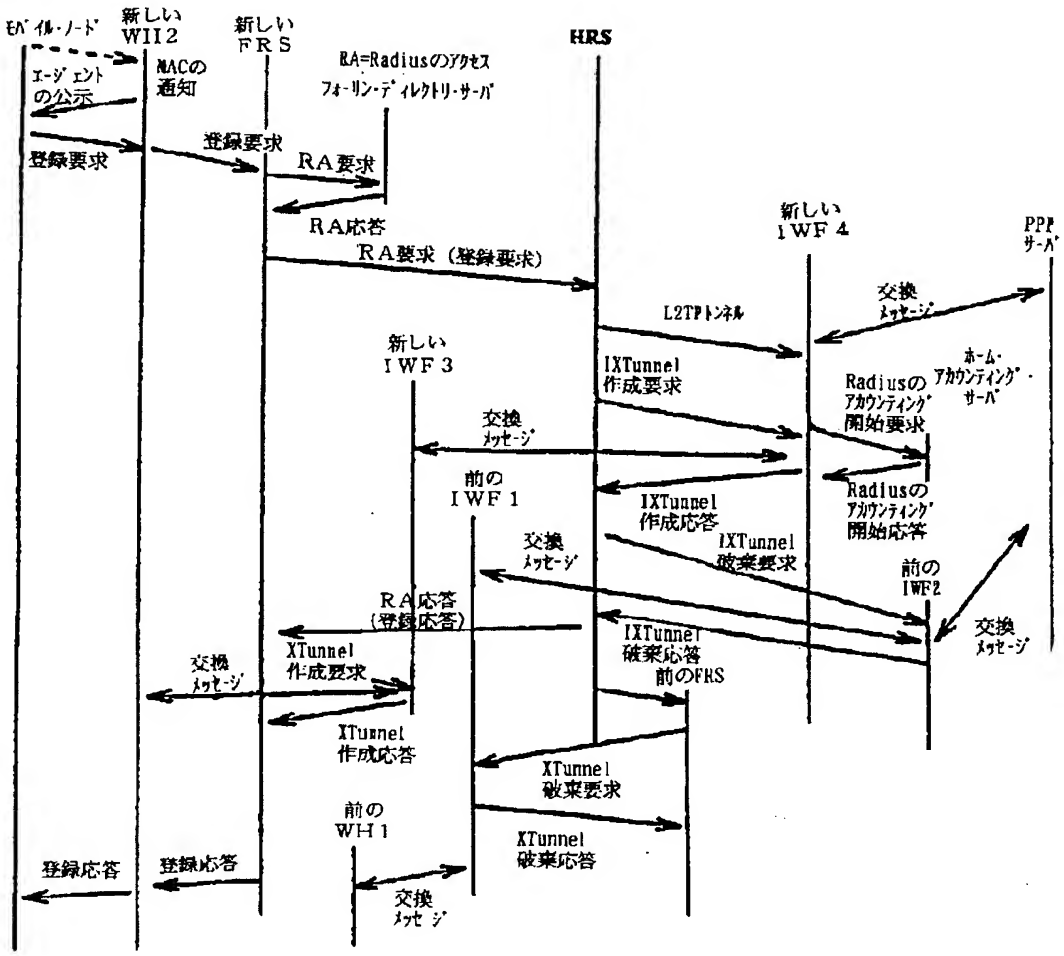
【図３５】


ﾓﾊﾞｲﾙ･ﾉｰﾄﾞ
新しい
WH２
FRS
RA=Radiusのｱｸｾｽ
ﾌｫｰﾘﾝ･ﾃﾞｨﾚｸﾄﾘ･ｻｰﾊﾞ
HRS
MACの
通知
ｴｰｼﾞｪﾝﾄ
の公示
登録要求
登録要求
RA要求
RA応答
RA要求
(登録要求)
ﾎｰﾑ･ﾃﾞｨﾚｸﾄﾘ･ｻｰﾊﾞ
RA要求
RA応答
新しい
IWF３
IXTunnel
作成要求
IWF2
Radiusの
ｱｶｳﾝﾃｨﾝｸﾞ
開始要求
ﾎｰﾑ･
ｱｶｳﾝﾃｨﾝｸﾞ
ｻｰﾊﾞ
交換
ﾒｯｾｰｼﾞ
前の
IWF1
IXTunnel
作成応答
Radiusの
ｱｶｳﾝﾃｨﾝｸﾞ
開始応答
IXTunnel
破棄要求
交換
ﾒｯｾｰｼﾞ
RA応答
(登録応答)
IXTunnel
破棄応答
交換
ﾒｯｾｰｼﾞ
XTunnel作成要求
XTunnel作成応答
XTunnel破棄要求
XTunnel破棄応答
前の
WH１
登録応答
登録応答
交換
ﾒｯｾｰｼﾞ

【図３６】


ﾓﾊﾞｲﾙ･ﾉｰﾄﾞ
新しい WH2
新しい FRS
HRS
MACの 通知
ｴｰｼﾞｪﾝﾄ の公示
RA=Radiusのｱｸｾｽ ﾌｫｰﾘﾝ･ﾃﾞｨﾚｸﾄﾘ･ｻｰﾊﾞ
登録要求
登録要求
RA要求
RA応答
RA要求 (登録要求)
ﾎｰﾑ･ﾃﾞｨﾚｸﾄﾘ･ｻｰﾊﾞ
RA要求
RA応答
新しい IWF3
IWF2
ﾎｰﾑ･ ｱｶｳﾝﾃｨﾝｸﾞ･ ｻｰﾊﾞ
Radiusの ｱｶｳﾝﾃｨﾝｸﾞ 更新要求
交換 ﾒｯｾｰｼﾞ
IXTunnel 作成要求
前の IWF1
Radiusの ｱｶｳﾝﾃｨﾝｸﾞ 更新応答
IXTunnel 作成応答
交換 ﾒｯｾｰｼﾞ
IXTunnel 破棄要求
RA応答 (登録応答)
IXTunnel 破棄応答
XTunnel 作成要求
交換 ﾒｯｾｰｼﾞ
前のFRS
XTunnel 作成応答
XTunnel 破棄要求
前の WH1
XTunnel 破棄応答
登録応答
登録応答
交換 ﾒｯｾｰｼﾞ

【図３７】



フロントページの続き

(51)Int.Cl.[6]		識別記号	FI		
H04L	12/56		H04L	11/00	310B
H04M	3/00				310C
	11/00	303		11/20	102Z

(72)発明者　ハイム　シャロム　ネア
アメリカ合衆国　07410　ニュージャーシィ，フェア　ハヴン，フェリー　ハイツ　36－05

(72)発明者　ギリシュ　ライ
アメリカ合衆国　60103　イリノイズ，バートレット，レディ　スミス　ロード　523

【外国語明細書】

1. Title of Invention

POINT-TO-POINT PROTOCOL ENCAPSULATION IN ETHERNET FRAME

2. Claims

1. A wireless data network comprising:

a home network that includes a home mobile switching center, a wireless modem and at least one end system, wherein said wireless modem and said at least one end system are connected together via an ethernet link; and

a PPP server, wherein PPP information sent from said PPP server for said at least one end system is encapsulated by the wireless modem in an ethernet frame and sent to said at least one end system via said ethernet link.

2. The network according to claim 1, wherein PPP information from said at least one end system is sent to the wireless modem via the ethernet link and then trnasmitted from the wireless modem to the PPP server.

3. The network according to claim 1, wherein said home switching center includes a home inter-working function.

4. The network according to claim 3, wherein PPP information from said PPP server is transmitted through the home inter-working function to the wireless modem.

5. The network according to claim 4, wherein PPP information from said at least one end system is sent to the wireless modem via the ethernet link and then transmitted from the wireless modem to the PPP server through the home inter-working function.

3. Detailed Explanation of the Invention

Background of the Invention

Priority benefit of the October 14, 1997 filing date of provisional application serial number 60/061,915 is hereby claimed.

Field of the Invention

The present invention relates to a wireless data network, and more particularly to communicating with a Pier to Pier Protocol server in the wireless data network.

Description Of Related Art

FIG. 1 depicts three business entities, whose equipment, working together typically provide remote internet access to user computers 2 through user modems 4. User computers 2 and modems 4 constitute end systems.

The first business entity is the telephone company (telco) that owns and operates the dial-up plain old telephone system (POTS) or integrated services data network (ISDN) network. The telco provides the media in the form of public switched telephone network (PSTN) 6 over which bits (or packets) can flow between users and the other two business entities.

The second business entity is the internet service provider (ISP). The ISP deploys and manages one or more points of presence (POPs) 8 in its service area to which end users connect for network service. An ISP typically establishes a POP in each major local calling area in which the ISP expects to subscribe customers. The POP converts message traffic from the PSTN run by the telco into a digital form to be carried over intranet backbone 10 owned by the ISP or leased from an intranet backbone provider like MCI, Inc. An ISP typically leases fractional or full T1 lines or fractional or full T3 lines from the telco for connectivity to the PSTN. The POPs and the ISP' medium data center 14 are connected together over the intranet backbone through router 12A. The data center houses the ISP's web servers, mail servers, accounting and registration servers, enabling the ISP to provide web content, e-mail and web hosting services to end users. Future value added services may be added by

deploying additional types of servers in the data center. The ISP also maintains router 12A to connect to public internet backbone 20. In the current model for remote access, end users have service relationships with their telco and their ISP and usually get separate bills from both. End users access the ISP, and through the ISP, public internet 20, by dialing the nearest POP and running a communication protocol known as the Internet Engineering Task Force (IETF) point-to-point protocol (PPP).

The third business entity is the private corporation which owns and operates its own private intranet 18 through router 12B for business reasons. Corporate employees may access corporate network 18 (e.g., from home or while on the road) by making POTS/ISDN calls to corporate remote access server 16 and running the IETF PPP protocol. For corporate access, end users only pay for the cost of connecting to corporate remote access server 16. The ISP is not involved. The private corporation maintains router 12B to connect an end user to either corporate intranet 18 or public internet 20 or both.

End users pay the telco for the cost of making phone calls and for the cost of a phone line into their home. End users also pay the ISP for accessing the ISP's network and services. The present invention will benefit wireless service providers like Sprint PCS, PrimeCo, etc. and benefit internet service providers like AOL, AT&T Worldnet, etc.

Today, internet service providers offer internet access services, web content services, e-mail services, content hosting services and roaming to end users. Because of low margins and no scope of doing market segmentation based on features and price, ISPs are looking for value added services to improve margins. In the short term, equipment vendors will be able to offer solutions to ISPs to enable them to offer faster access, virtual private networking (which is the ability to use public networks securely as private networks and to connect to intranets), roaming consortiums, push technologies and quality of service. In the longer term, voice over internet and mobility will also be offered. ISPs will use these value added services to escape from the low margin straitjacket. Many of these value added services fall in the category of network services and can be offered only through the network

infrastructure equipment. Others fall in the category of application services which require support from the network infrastructure, while others do not require any support from the network infrastructure. Services like faster access, virtual private networking, roaming, mobility, voice, quality of service, quality of service based accounting all need enhanced network infrastructure. The system described here will be either directly provide these enhanced services or provide hooks so that these services can be added later as future enhancements. Wireless service providers will be able to capture a larger share of the revenue stream. The ISP will be able to offer more services and with better market segmentation.

Summary Of The Invention

The present invention provides end users with remote wireless access to the public internet, private intranets and internet service providers. Wireless access is provided through base stations in a home network and base stations in foreign networks with interchange agreements.

It is an object of the present system to provide a wireless packet switched data network for end users that divides mobility management into local, micro, macro and global connection handover categories and minimizes handoff updates according to the handover category. It is another object to integrate MAC handoff messages with network handoff messages. It is a further object of the present system to separately direct registration functions to a registration server and direct routing functions to inter-working function units. It is yet another object to provide an intermediate XTunnel channel between a wireless hub (also called access hub AH) and an inter-working function unit (IWF unit) in a foreign network. It is yet another object to provide an IXTunnel channel between an inter-working function unit in a foreign network and an inter-working function unit in a home network. It is yet another object to enhance the layer two tunneling protocol (L2TP) to support a mobile end system. It is yet another object to perform network layer registration before the start of a PPP communication session.

According to one embodiment of the invention, a wireless data network which provides communications with a Pier to Pier Protocol server is disclosed. The

network includes a home network that includes a home mobile switching center, a wireless modem and one or more end system. The wireless modem and the end systems are connected together via an ethernet link. The network also includes a PPP server, wherein PPP information sent from PPP server for the end systems is encapsulated by the wireless modem in an ethernet frame and sent to the end systems via the ethernet link.

Detailed Description Of Preferred Embodiments

The present system provides computer users with remote access to the internet and to private intranets using virtual private network services over a high speed, packet switched, wireless data link. These users are able to access the public internet, private intranets and their internet service providers over a wireless link. The network supports roaming, that is, the ability to access the internet and private intranets using virtual private network services from anywhere that the services offered by the present system are available. The network also supports handoffs, that is, the ability to change the point of attachment of the user to the network without disturbing the PPP link between the PPP client and the PPP server. The network targets users running horizontal internet and intranet applications. These applications include electronic mail, file transfer, browser based WWW access and other business applications built around the internet. Because the network will be based on the IETF standards, it is possible to run streaming media protocols like RTP and conferencing protocols like H.323 over it.

Other internet remote access technologies that are already deployed or are in various stages of deployment include: wire line dial-up access based on POTS and ISDN, XDSL access, wireless circuit switched access based on GSM/CDMA/TDMA, wireless packet switched access based on GSM/CDMA/TDMA, cable modems, and satellite based systems. However, the present system offers a low cost of

deployment, ease of maintenance, a broad feature set, scaleability, an ability to degrade gracefully under heavy load conditions and support for enhanced network services like virtual private networking, roaming, mobility and quality of service to the relative benefit of users and service providers.

For wireless service providers who own personal communications system (PCS) spectrum, the present system will enable them to offer wireless packet switched data access services that can compete with services provided by the traditional wire line telcos who own and operate the PSTN. Wireless service providers may also decide to become internet service providers themselves, in which case, they will own and operate the whole network and provide end to end services to users.

For internet service providers the present system will allow them to by-pass the telcos (provided they purchase or lease the spectrum) and offer direct end to end services to users, perhaps saving access charges to the telcos, which may increase in the future as the internet grows to become even bigger than it is now.

The present systems flexible so that it can benefit wireless service providers who are not internet service providers and who just provide ISP, internet or private intranet access to end users. The system can also benefit service providers who provide wireless access and internet services to end users. The system can also benefit service providers who provide wireless access and internet services but also allow the wireless portion of the network to be used for access to other ISPs or to private intranets.

In FIG. 2, end systems 32 (e.g., based on, for example, Win 95 personal computer) connect to wireless network 30 using external or internal modems. These modems allow end systems to send and receive medium access control (MAC) frames over air link 34. External modems attach to the PC via a wired or wireless link. External modems are fixed, and, for example, co-located with roof top mounted directional antennae. External modems may be connected to the user's PC using any one of following means: 802.3, universal serial bus, parallel port, infra-red, or even an ISM radio link. Internal modems are preferably PCMCIA cards for laptops and are plugged into the laptop's backplane. Using a small omni-directional antenna, they

send and receive MAC frames over the air link. End systems can also be laptops with a directional antenna, a fixed wireless station in a home with a directional antenna connected via AC lines, and other alternatives.

Wide-area wireless coverage is provided by base stations 36. The base station 36 can employ a 5-channel reuse communication scheme as described in U.S. Patent Application Serial No. 08/998,505, filed on December 26, 1997. The range of coverage provided by base stations 36 depends on factors like link budget, capacity and coverage. Base stations are typically installed in cell sites by PCS (personal communication services) wireless service providers. Base stations multiplex end system traffic from their coverage area to the system's mobile switching center (MSC) 40 over wire line or microwave backhaul network 38.

The system is independent of the MAC and PHY (physical) layer of the air link and the type of modem. The architecture is also independent of the physical layer and topology of backhaul network 38. The only requirements for the backhaul network are that it must be capable of routing internet protocol (IP) packets between base stations and the MSC with adequate performance. At Mobile Switching Center 40 (MSC 40), packet data inter-working function (IWF) 52 terminates the wireless protocols for this network. IP router 42 connects MSC 40 to public internet 44, private intranets 46 or to internet service providers 46. Accounting and directory servers 48 in MSC 40 store accounting data and directory information. Element management server 50 manages the equipment which includes the base stations, the IWFs and accounting/directory servers.

The accounting server will collect accounting data on behalf of users and send the data to the service provider's billing system. The interface supported by the accounting server will send accounting information in American Management Association (AMA) billing record format, or any other suitable billing format, over a TCP/IP (transport control protocol/internet protocol) transport to the billing system (which is not shown in the figure).

The network infrastructure provides PPP (point-to-point protocol) service to end systems. The network provides (1) fixed wireless access with roaming (log-in

anywhere that the wireless coverage is available) to end systems and (2) low speed mobility and hand-offs. When an end system logs on to a network, in it may request either fixed service (i.e., stationary and not requiring handoff services) or mobile service (i.e., needing handoff services). An end system that does not specify fixed or mobile is regarded as specifying mobile service. The actual registration of the end system is the result of a negotiation with a home registration server based on requested level of service, the level of services subscribed to by the user of the end system and the facilities available in the network.

If the end system negotiates a fixed service registration (i.e., not requiring handoff services) and the end system is located in the home network, an IWF (inter-working function) is implemented in the base station to relay traffic between the end user and a communications server such as a PPP server (i.e., the point with which to be connected, for example, an ISP PPP server or a corporate intranet PPP server or a PPP server operated by the wireless service provider to provide customers with direct access to the public internet). It is anticipated that perhaps 80% of the message traffic will be of this category, and thus, this architecture distributes IWF processing into the base stations and avoids message traffic congestion in a central mobile switching center.

If the end system requests mobile service (from a home network or a foreign network) or if the end system request roaming service (i.e., service from the home network through a foreign network), two IWFs are established: a serving IWF typically established in the base station of the network to which the end system is attached (be it the home network or a foreign network) and a home IWF typically established in mobile switching center MSC of the home network. Since this situation is anticipated to involve only about 20% of the message traffic, the message traffic congestion around the mobile switching center is minimized. The serving IWF and the wireless hub may be co-located in the same nest of computers or may even be programmed in the same computer so that a tunnel using an XTunnel protocol need not be established between the wireless hub and the serving IWF.

However, based on available facilities and the type and quality of service requested, a serving IWF in a foreign network may alternatively be chosen from facilities in the foreign MSC. Generally, the home IWF becomes an anchor point that is not changed during the communications session, while the serving IWF may change if the end system moves sufficiently.

The base station includes an access hub and at least one access point (be it remote or collocated with the access hub). Typically, the access hub serves multiple access points. While the end system may be attached to an access point by a wire or cable according to the teachings of this invention, in a preferred embodiment the end system is attached to the access point by a wireless "air link", in which case the access hub is conveniently referred to as a wireless hub. While the access hub is referred to as a "wireless hub" throughout the description herein, it will be appreciated that an end system coupled through an access point to an access hub by wire or cable is an equivalent implementation and is contemplated by the term "access hub".

In the invention, an end system includes an end user registration agent (e.g., software running on a computer of the end system, its modem or both) that communicates with an access point, and through the access point to a wireless hub. The wireless hub includes a proxy registration agent (e.g., software running on a processor in the wireless hub) acting as a proxy for the end user registration agent. Similar concepts used in, for example, the IETF proposed Mobile IP standard are commonly referred to as a foreign agent (FA). For this reason, the proxy registration agent of the present system will be referred to as a foreign agent, and aspects of the foreign agent of the present system that differ from the foreign agent of Mobile IP are as described throughout this description.

Using the proxy registration agent (i.e., foreign agent FA) in a base station, the user registration agent of an end system is able to discover a point of attachment to the network and register with a registration server in the MSC (mobile switching center) of the home network. The home registration server determines the availability of each of the plural inter-working function modules (IWFs) in the network (actually

software modules that run on processors in both the MSC and the wireless hubs) and assigns IWF(s) to the registered end system. For each registered end system, a tunnel (using the *XTunnel* protocol) is created between the wireless hub in the base station and an inter-working function (IWF) in the mobile switching center (MSC), this tunnel transporting PPP frames between the end system and the IWF.

As used herein, the XTunnel protocol is a protocol that provides in-sequence transport of PPP data frames with flow control. This protocol may run over standard IP networks or over point-to-point networks or over switched networks like ATM data networks or frame relay data networks. Such networks may be based on T1 or T3 links or based on radio links, whether land based or space based. The XTunnel protocol may be built by adapting algorithms from L2TP (level 2 transport protocol). In networks based on links where lost data packets may be encountered, a re-transmission feature may be a desirable option.

The end system's PPP peer (i.e., a communications server) may reside in the IWF or in a corporate intranet or ISP's network. When the PPP peer resides in the IWF, an end system is provided with direct internet access. When the PPP peer resides in an intranet or ISP, an end system is provided with intranet access or access to an ISP. In order to support intranet or ISP access, the IWF uses the layer two tunneling protocol (L2TP) to connect to the intranet or ISP's PPP server. From the point of view of the intranet or ISP's PPP server, the IWF looks like a network access server (NAS). PPP traffic between the end system and the IWF is relayed by the foreign agent in the base station.

In the reverse (up link) direction, PPP frames traveling from the end system to the IWF are sent over the MAC and air link to the base station. The base station relays these frames to the IWF in the MSC using the *XTunnel* protocol. The IWF delivers them to a PPP server for processing. For internet access, the PPP server may be in the same machine as the IWF. For ISP or intranet access, the PPP server is in a private network and the IWF uses the layer two tunneling protocol (L2TP) to connect to it.

In the forward (down link) direction, PPP frames from the PPP server are relayed by the IWF to the base station using the *XTunnel* protocol. The base station de-tunnels down link frames and relays them over the air link to the end system, where they are processed by the end system's PPP layer.

To support mobility, support for hand-offs are included. The MAC layer assists the mobility management software in the base station and the end system to perform hand-offs efficiently. Hand-offs are handled transparently from the peer PPP entities and the L2TP tunnel. If an end system moves from one base station to another, a new *XTunnel* is created between the new base station and the original IWF. The old *XTunnel* from the old base station will be deleted. PPP frames will transparently traverse the new path.

The network supports roaming (i.e., when the end user connects to its home wireless service provider through a foreign wireless service provider). Using this feature, end systems are able to roam away from the home network to a foreign network and still get service, provided of course that the foreign wireless service provider and the end system's home wireless service provider have a service agreement.

In FIG. 3, roaming end system 60 has traveled to a location at which foreign wireless service provider 62 provides coverage. However, roaming end system 60 has a subscriber relationship with home wireless service provider 70. In the present invention, home wireless service provider 70 has a contractual relationship with foreign wireless service provider 62 to provide access services. Therefore, roaming end system 60 connects to base station 64 of foreign wireless service provider 62 over the air link. Then, data is relayed from roaming end system 60 through base station 64, through serving IWF 66 of foreign wireless service provider 62, to home IWF 72 of home wireless service provider 70, or possibly through home IWF 72 of home wireless service provider 70 to internet service provider 74.

An inter-service provider interface, called the I-interface, is used for communications across wireless service provider (WSP) boundaries to support

roaming. This interface is used for authenticating, registering and for transporting the end system's PPP frames between the foreign WSP and the home WSP.

PPP frames in the up link and the down link directions travel through the end system's home wireless service provider (WSP). Alternatively, PPP frames directly transit from the foreign WSP to the destination network. The base station in the foreign WSP is the end system's point of attachment in the foreign network. This base station sends (and receives) PPP frames to (and from) a serving IWF in the foreign WSP's mobile switching center. The serving IWF connects over the I-interface to the home IWF using a layer two tunnel to transport the end system's PPP frames in both directions. The serving IWF in the foreign WSP collects accounting data for auditing. The home IWF in the home WSP collects accounting data for billing.

The serving IWF in the foreign WSP may be combined with the base station in the same system, thus eliminating the need for the X-Tunnel.

During the registration phase, a registration server in the foreign WSP determines the identity of the roaming end system's home network. Using this information, the foreign registration server communicates with the home registration server to authenticate and register the end system. These registration messages flow over the I-interface. Once the end system has been authenticated and registered, a layer two tunnel is created between the base station and the serving IWF using the *XTUNNEL* protocol and another layer two tunnel is created between the serving IWF and the home IWF over the I-interface. The home IWF connects to the end system's PPP peer as before, using L2TP (level 2 tunnel protocol). During hand-offs, the location of the home IWF and the L2TP tunnel remains fixed. As the end system moves from one base station to another base station, a new tunnel is created between the new base station and the serving IWF and the old tunnel between the old base station and the serving IWF is deleted. If the end system moves far enough, so that a new serving IWF is needed, a new tunnel will be created between the new serving IWF and the home IWF. The old tunnel between the old serving and the home will be deleted.

To support roaming, the I-interface supports authentication, registration and data transport services across wireless service provider boundaries. Authentication and registration services are supported using the IETF Radius protocol. Data transport services to transfer PPP frames over a layer two tunnel are supported using the *I-XTunnel* protocol. This protocol is based on the IETF L2TP protocol.

As used in this description, the term home IWF refers to the IWF in the end system's home network. The term serving IWF refers to the IWF in the foreign network which is temporarily providing service to the end system. Similarly, the term home registration server refers to the registration server in the end system's home network and the term foreign registration server refers to the registration server in the foreign network through which the end system registers while it is roaming.

The network supports both fixed and dynamic IP address assignment for end systems. There are two types of IP addresses that need to be considered. The first is the identity of the end system in its home network. This may be a structured user name in the format user@domain. This is different from the home IP address used in mobile IP. The second address is the IP address assigned to the end system via the PPP IPCP address negotiation process. The domain sub-field of the home address is used to identify the user's home domain and is a fully qualified domain name. The user sub-field of the home address is used to identify the user in the home domain. The User-Name is stored on the end system and in the subscriber data-base at the MSC and is assigned to the user when he or she subscribes to the service. The domain sub-field of the User-Name is used during roaming to identify roaming relationships and the home registration server for purposes of registration and authentication. Instead of the structured user name another unique identifier may be used to identify the user's home network and the user's identity in the home network. This identifier is sent in the registration request by the end system

The PPP IPCP is used to negotiate the IP address for the end system. Using IP configuration protocol IPCP, the end system is able to negotiate a fixed or dynamic IP address.

Although the use of the structured user-name field and the non-use of an IP address as the home address is a feature that characterizes the present system over a known mobile IP, the network may be enhanced to also support end systems that have no user-name and only a non-null home address, if mobile IP and its use in conjunction with PPP end systems becomes popular. The PPP server may be configured by the service provider to assign IP addresses during the IPCP address assignment phase that are the same as the end system's home IP address. In this case, the home address and the IPCP assigned IP address will be identical.

In FIG. 4, base station 64 and air links from end systems form wireless sub-network 80 that includes the air links for end user access, at least one base station (e.g., station 64) and at least one backhaul network (e.g., 38 of FIG. 2) from the base station to MSC 40 (FIG.2). The wireless sub-network architecture of, for example, a 3-sectored base station includes the following logical functions.

1. *Access point function.* Access points 82 perform MAC layer bridging and MAC layer association and dissociation procedures. An access point includes a processor (preferably in the form of custom application specific integrated circuit ASIC), a link to a wireless hub (preferably in the form of an Ethernet link on a card or built into the ASIC), a link to an antenna (preferably in the form of a card with a data modulator/demodulator and a transmitter/receiver), and the antenna to which the end system is coupled. The processor runs software to perform a data bridging function and various other functions in support of registration and mobility handovers as further described herein. See discussion with respect to FIGS. 7, 8 and 11.

   Access points (APs) take MAC layer frames from the air link and relay them to a wireless hub and vice versa. The MAC layer association and disassociation procedures are used by APs to maintain a list of end system MAC addresses in their MAC address filter table. An AP will only perform MAC layer bridging on behalf of end systems whose MAC addresses are present in the table. An access

point and its associated wireless hub are typically co-located. In its simplest form, an access point is just a port into a wireless hub. When the APs and the wireless hub are co-located in the same cell site, they may be connected together via a IEEE 802.3 link. Sometimes, access points are located remotely from the wireless hub and connected via a long distance link like a wired T1 trunk or even a wireless trunk. For multi-sector cells, multiple access points (i.e., one per sector) are used.

2. *Wireless hub function.* Wireless hub 84 performs the foreign agent (FA) procedures, backhaul load balancing (e.g., over multiple T1's), backhaul network interfacing, and the *xtunnel* procedures. When support for quality of service (QOS) is present, the wireless hub implements the support for QOS by running the *xtunnel* protocol over backhauls with different QOS attributes. In a multi-sector cell site, a single wireless hub function is typically shared by multiple access points.

A wireless hub includes a processor, a link to one or more access points (preferably in the form of an Ethernet link on a card or built into an ASIC), and a link to a backhaul line. The backhaul line is typically a T1 or T3 communications line that terminates in the mobile switching center of the wireless service provider. The link to the backhaul line formats data into a preferred format, for example, an Ethernet format, a frame relay format or an ATM format. The wireless hub processor runs software to support data bridging and various other functions as described herein. See discussion with respect to FIGS. 9, 10 and 11.

The base station design supports the following types of cell architectures.

1. *Local AP architecture.* In a local AP architecture, access points have a large (> = 2km, typically) range. They are co-located in the cell site with the wireless hub (FIG. 4). Access points may be connected

to the wireless hub using an IEEE 802.3 network or may be directly plugged into the wireless hub's backplane or connected to the wireless hub using some other mechanism (e.g. universal serial bus, printer port, infra-red, etc.). It will be assumed that the first alternative is used for the rest of this discussion. The cell site may be omni or sectored by adding multiple access points and sectored antennas to a wireless hub.

2. *Remote AP architecture.* In a remote AP architecture, access points usually have a very small range, typically around 1 km radius. They are located remotely (either indoors or outdoors) from the wireless hub. A T1 or a wireless trunk preferably links remote access points to the cell site where the wireless hub is located. From the cell site, a wire line backhaul or a microwave link is typically used to connect to the IWF in the MSC. If wireless trunking between the remote AP and the wireless hub is used, omni or sectored wireless radios for trunking are utilized. The devices for trunking to remote access points are preferably co-located with the wireless hub and may be connected to it using an IEEE 802.3 network or may be directly plugged into the wireless hub's backplane. These devices will be referred to by the term trunk AP.

3. *Mixed AP architecture.* In a mixed architecture, the wireless sub-network will have to support remote and local access points. Remote access points may be added for hole filling and other capacity reasons. As described earlier, T1 or wireless trunks may be used to connect the remote AP to the wireless hub.

FIG. 5 shows a cell with three sectors using local APs only. The access points and the wireless hub are co-located in the base station and are connected to each other with 802.3 links.

FIG. 6 shows an architecture with remote access points 82 connected to wireless hub 84 using wireless trunks 86. Each trunk access point in the base station

provides a point to multi-point wireless radio link to the remote micro access points (R-AP in figure). The remote access points provide air link service to end systems. The wireless hub and the trunk access points are co-located in the base station and connected together via 802.3 links. This figure also shows remote access points 82R connected to the wireless hub via point to point T1 links. In this scenario, no trunk APs are required.

To support all of the above cell architectures and the different types of access points that each cell might use, the network architecture follows the following rules:

1. Access points function as MAC layer bridges. Remote access points perform MAC bridging between the air link to the end systems and the wireless or T1 trunk to the cell site. Local access points perform MAC bridging between the air link to the end systems and the wireless hub.

2. Trunk access points also function as MAC layer bridges. They perform MAC bridging between the trunk (which goes to the access points) and the wireless hub.

3. The wireless hub is connected to all co-located MAC bridges (i.e. local access points or trunk access points) using a 802.3 link initially.

Additionally, where local access points or remote access points with T1 trunks are used, the following rules are followed.

1. Local access points are co-located with the wireless hub and connected to it using point to point 802.3 links or a shared 802.3 network. Remote access points are connected to the wireless hub using point to point T1 trunks.

2. Sectorization is supported by adding access points with sectored antennas to the cell site.

3. For each access point connected to the wireless hub, there is a foreign agent executing in the wireless hub which participates in end

system registration. MAC layer association procedures are used to keep the MAC address filter tables of the access points up to date and to perform MAC layer bridging efficiently. The wireless hub participates in MAC association functions so that only valid MAC addresses are added to the MAC address filter tables of the access points.

4. The foreign agent in the wireless hub relays frames from the access points to the MSC IWF and vice versa using the *xtunnel* protocol. The MAC address filter table is used to filter out those unicast MAC data frames whose MAC addresses are not present in the table. The APs always forward MAC broadcast frames and MAC frames associated with end system registration functions regardless of the contents of the MAC address filter table.

5. Local access points use ARP to resolve MAC addresses for routing IP traffic to the wireless hub. Conversely, the wireless hub also uses ARP to route IP packets to access points. UDP/IP is used for network management of access points.

6. Remote access points connected via T1 do not use ARP since the link will be a point to point link.

7. Support for hand-offs is done with assistance from the MAC layer.

In a cell architecture using wireless trunks and trunk APs, the following rules are followed.

1. Trunk access points are co-located with the wireless hub and connected to it using point to point 802.3 links or other suitable means.

2. Wireless trunk sectorization is supported by adding trunk access points with sectored antennas to the cell site.

3. Hand-offs across backhaul sectors are done using the foreign agent in the wireless hub. For each backhaul sector, there is a foreign agent executing in the wireless hub.

4. The trunk APs do not need to participate in MAC layer end system association and hand off procedures. Their MAC address filter tables will be dynamically programmed by the wireless hub as end systems register with the network. The MAC address filter table is used to filter out unicast MAC frames. Broadcast MAC frames or MAC frames containing registration packets are allowed to always pass through.

5. Trunk APs use ARP to resolve MAC addresses for routing IP traffic to the wireless hub. Conversely, the wireless hub use ARP to route IP packets to trunk APs. UDP/IP is used for network management of trunk APs.

6. In a single wireless trunk sector, MAC association and hand-offs from one access point to another is done using the MAC layer with the assistance of the foreign agent in the wireless hub. Using these MAC layer procedures, end systems associate with access points. As end systems move from one access point to another access point, the access points will use a MAC hand off protocol to update their MAC address filter tables. The wireless hub at the cell site provides assistance to access points to perform this function. This assistance includes relaying MAC layer hand off messages (since access points will not be able to communicate directly over the MAC layer with each other) and authenticating the end system for MAC layer registration and hand off and for updating the MAC address filter tables of the access points.

7. The foreign agent for a wireless trunk sector is responsible for relaying frames from its trunk AP to the MSC and vice versa using the *xtunnel* protocol. Thus, the foreign agent for a trunk AP does

not care about the location of the end system with respect to access points within that wireless trunk sector. In the down link direction, it just forwards frames from the tunnel to the appropriate trunk AP which uses MAC layer bridging to send the frames to all the remote access points attached in that backhaul sector. The access points consult their MAC address filter tables and either forward the MAC frames over the access network or drop the MAC frames. As described above, the MAC address filter tables are kept up to date using MAC layer association and hand off procedures. In the up link direction, MAC frames are forwarded by the access points to the backhaul bridge which forwards them to the foreign agent in the wireless hub using the 802.3 link.

8. ARP is not be used for sending or receiving IP packets to the remote access points. The access points determines the MAC address of the wireless hub using BOOTP procedures. Conversely, the wireless hub is configured with the MAC address of remote access points. UDP/IP is used for network management of access points and for end system association and hand off messages.

IEEE Standard 802.3 links in the cell site may be replaced by other speed links.

FIG. 7 shows the protocol stack for a local access point. At the base of the stack is physical layer PHY. Physical layer PHY carries data to and from an end system over the air using radio waves as an example. When received from an end system, the AP receives data from the physical layer and unpacks it from the MAC frames (the MAC layer). The end system data frames are then repacked into an Ethernet physical layer format (IEEE 802.3 format) where it is send via the Ethernet link to the wireless hub. When the AP's processor receives data from the wireless hub via its Ethernet link (i.e., the physical layer), the data to be transmitted to an end system, the AP packs the data in a medium access control

(MAC) format, and sends the MAC layer data to its modulator to be transmitted to the end system using the PHY layer.

In FIG. 8, the MAC and PHY layers to/from the end system of FIG. 7 are replaced by a MAC and PHY for the trunk to the cell site for a remote access point. Specifically, for a T1 trunk, the high level data link control protocol (HDLC protocol) is preferably used over the T1.

FIG. 9 depicts the protocol stack for the wireless hub that bridges the backhaul line and the trunk to the remote access point. The trunk to the remote APs are only required to support remote access points (as distinct from Ethernet coupled access points). The MAC and PHY layers for the wireless trunk to the remote APs provide a point to multipoint link so that one trunk may be used to communicate with many remote APs in the same sector.

The wireless hub bridges the trunk to the remote APs and the backhaul line (e.g., T1 or T3) to the network's mobile switching center (MSC). The protocol stack in the wireless hub implements MAC and PHY layers to the MSC on top of which is implemented an IP (Internet Protocol) layer on top of which is implemented a UDP layer (Universal Datagram Protocal, in combination referred to as UDP/IP) for network management on top of which is implemented an XTunnel protocol. The XTunnel protocol is a new format that includes aspects of mobility (e.g. as in mobile IP) and aspects of the Level 2 Tunnel Protocol (L2TP). The XTunnel protocol is used to communicate from the wireless hub to the MSC and between inter-working functions (IWFs) in different networks or the same network.

In FIG. 10, the protocol stack for the relay function in the base station for supporting remote access points is shown. The relay function includes an interface to the backhaul line (depicted as the wireless hub) and an interface to the remote AP (depicted as a trunk AP). From the point of view of the wireless hub, the trunk AP (depicted in FIGS. 7 and 10) actually behaves like the AP depicted in FIG. 7. Preferably, the base station protocol stacks are split up into a wireless

hub and a trunk AP with an Ethernet in between. In an N-sector wireless trunk, there are N wireless trunk APs in the cell site and one wireless hub.

In FIG. 11, the base station protocol stack for a cell architecture using a local AP is shown. The relay function includes an interface to the backhaul line (depicted as the wireless hub) and an air link interface to the end system (depicted as an AP). From the point of view of the wireless hub, the AP (depicted in FIGS. 8 and 11) actually behaves like the trunk AP depicted in FIG. 8. Preferably, the base station protocol stacks are split up into a wireless hub and a trunk AP with an Ethernet in between. In a N-sector cell, there are N access points and a single wireless hub.

The backhaul network from the base station to the MSC has the following attributes.

1. The network is capable of routing IP datagrams between the base station and the MSC.

2. The network is secure. It is not a public internet. Traffic from trusted nodes only are allowed onto the network since the network will be used for not only transporting end system traffic, but also for transporting authentication, accounting, registration and management traffic.

3. The network has the necessary performance characteristics.

In typical application, the service provider is responsible for installing and maintaining the backhaul network on which the equipment is installed.

The base stations supports the following backhaul interfaces for communicating with the MSC.

1. Base stations support IP over PPP with HDLC links using point to point T1 or fractional T3 links.

2. Base stations support IP over frame relay using T1 or fractional T3 links.

3. Base stations support IP over AAL5/ATM using T1 or fractional T3 links.

4. Base stations support IP over Ethernet links.

Since all of the above interfaces are based on IETF standard encapsulations, commercial routers may be used in the MSC to terminate the physical links of the backhaul network. Higher layers are passed on and processed by the various servers and other processors.

End system registration procedures above the MAC layer are supported. In the following, end system registration procedures at the MAC layer are ignored except where they impact the layers above.

End systems may register for service on their home network or from a foreign network. In both scenarios, the end system uses a foreign agent (FA) in the base station to discover a point of attachment to the network and to register. In the former case, the FA is in the end system's home network. In the latter case, the FA is in a foreign network. In either case, the network uses an IWF in the end system's home network as an anchor point (i.e., unchanging throughout the session in spite of mobility). PPP frames to and from the end system travel via the FA in the base station to the IWF in the home network. If the end system is at home, the home IWF is directly connected by means of the *xtunnel* protocol to the base station. Note that the home IWF may be combined with the base station in the same node. If the end system is roaming, a serving IWF in the foreign network is connected to the home IWF over an I-interface. The serving IWF relays frames between the base station and the home IWF. Note that the home IWF may be combined with the base station in the same node. From the home IWF, data is sent to a PPP server which may reside in the same IWF or to a separate server using the L2TP protocol. The separate server may be owned and operated by a private network operator (e.g. ISP or corporate intranet) who is

different from the wireless service provider. For the duration of the session, the location of the home IWF and the PPP server remains fixed. If the end system moves while connected, it will have to re-register with a new foreign agent. However, the same home IWF and PPP server continues to be used. A new *xtunnel* is created between the new FA and the IWF and the old *xtunnel* between the old foreign agent and the IWF is destroyed.

FIG. 12 shows this network configuration for two end systems A and B, both of whose home wireless network is wireless service provider A (WSP-A). One end system is registered from the home wireless network and the other from a foreign wireless network. The home IWF in WSP-A serves as the anchor point for both end systems. For both end systems, data is relayed to the home IWF. The home IWF connects to an internet service provider's PPP server owned by ISP-A. Here it is assumed that both end systems have subscribed to the same ISP. If that were not the case, then the home IWF would be shown also connected to another ISP.

Within a wireless service providers network, data between base stations and the IWF is carried using the *xtunnel* protocol. Data between the IWF and the PPP server is carried using Level 2 Tunneling Protocol (L2TP). Data between the serving IWF and the home IWF is carried using the *I-xtunnel protocol*.

In a simple scenerio, for a user in their home network requiring fixed service, the home IWF function may be dynamically activated in the base station. Also, the serving IWF function may be activated for a roaming user in the base station.

Always using an IWF in the home network has its advantages and disadvantages. An obvious advantage is simplicity. A disadvantage is that of always having to relay data to and from a possibly remote home IWF. The alternative is to send all the necessary information to the serving IWF so that it may connect to the end system's ISP/intranet and for the serving IWF to send accounting information in near real time back to the accounting server in the home network. This functionality is more complex to implement, but more efficient

because it reduces the need to relay data over potentially long distances from the foreign network to the home network.

For example, consider a case of a user who roams from Chicago to Hong Kong. If the user's home network is in Chicago and the user registers using a wireless service provider in Hong Kong, then in the first configuration, the anchor point will be the home IWF in Chicago and all data will have to be relayed from Hong Kong to Chicago and vice versa. The home IWF in Chicago will connect to the user's ISP in Chicago. With the second configuration, the end system user will be assigned an ISP in Hong Kong. Thus, data will not always have to be relayed back and forth between Chicago and Hong Kong. In the second configuration, the serving IWF will serve as the anchor and never change for the duration of the session even if the end system moves. However, the location of the FA may change as a result of end system movement in Hong Kong.

FIG. 13 shows the second network configuration. In this figure, the home network for end system A and B is WSP-A. End system A registers from its home network, using its home IWF as an anchor point, and also connects to its ISP-A using the ISPs PPP server. End system B registers from the foreign network of WSP-B and uses a serving IWF which serves as the anchor point and connects the end system to an ISP using the ISP's PPP server. In this configuration, data for end system B does not have to be relayed from the foreign network to the home network and vice versa.

In order for this configuration to work, not only must there be roaming agreements between the home and the foreign wireless service providers, but there also must be agreements between the foreign wireless service provider and the end system's internet service provider directly or through an intermediary. In the example above, not only must the wireless service provider in Hong Kong have a business agreement with the wireless service provider in Chicago, but the WSP in Hong Kong must have a business agreement with the user's Chicago ISP and access to the Chicago ISPs PPP server in Hong Kong or a business agreement with another ISP locally in Hong Kong who has a business agreement for roaming with

the user' Chicago ISP. Additionally, the WSP in Hong Kong must be able to discover these roaming relationships dynamically in order to do user authentication and accounting and to set up the appropriate tunnels.

It is difficult for those companies who are in the Internet infrastructure business to work out suitable standards in the IETF for all of these scenarios. Thus, a preferable embodiment for the present systems to implement the simpler, potentially less efficient configuration, where the IWF in the home network is always used as the anchor point. However, in the presence of suitable industry standardization of protocols for Internet roaming, the second configuration should be regarded as equivalent or alternative embodiment.

An end system will have to register with the wireless network before it can start PPP and send and receive data. The end system first goes through the FA discovery and registration phases. These phases authenticate and register the end system to the wireless service provider. Once these phases are over, the end system starts PPP. This includes the PPP link establishment phase, the PPP authentication phase and the PPP network control protocol phase. Once these phases are over, the end system is able to send and receive IP packets using PPP.

The following discussion assumes that the end system is roaming and registering from a foreign network. During the FA discovery phase, the end system (through its user registration agent) waits for or solicits an advertisement from the foreign agent. The user registration agent uses advertisement messages sent by a near by foreign agent to discover the identity of the FA and to register. During this phase, the user registration agent of the end system selects a FA and issues a registration request to it. The FA acting as a proxy registration agent forwards the registration request to its registration server (the registration server in the foreign WSP). The registration server uses User-Name from the user registration agent's request to determine the end system's home network, and forwards the registration request for authentication to a registration server in the home network. Upon receiving the registration request relayed by the foreign registration server, the home registration server authenticates the identity of the

foreign registration server and also authenticates the identity of the end system. If authentication and registration succeeds, the home registration server selects an IWF in the home network to create an *I-xtunnel* link between the home IWF and the serving IWF (in the foreign WSP). The IWF in the home network serves as the anchor point for the duration of the PPP session.

Once the authentication and registration phases are over, the various PPP phases will be started. At the start of PPP, an L2TP connection is created between the home IWF and requested ISP/intranet PPP server. In the PPP authentication phase, PPP passwords using Password Authentication Protocol (PAP) or Challenge Authentication Protocol CHAP are exchanged and the ISP or intranet PPP server independently authenticates the identity of the end system.

Once this succeeds, the PPP network control phase is started. In this phase, an IP address is negotiated and assigned to the end system by the PPP server and the use of TCP/IP header compression is also negotiated. When this is complete, the end system is able to send and receive IP packets using PPP to its ISP or a corporate intranet.

Note that two levels of authentication are performed. The first authentication authenticates the identity of the end system to the registration server in the home network and the identities of the foreign network and the home network to each other. To perform this function, the foreign agent forwards the end system's registration request using, for example, an IETF Radius protocol to a registration server in its local MSC in a Radius Access-Request packet. Using the end system's domain name, the foreign registration server determines the identity of the end system's home network and home registration server, and acting as a Radius proxy, encapsulates and forwards the request to the end system's home registration server. If the foreign registration server cannot determine the identity of the end system's home, it may optionally forward the Radius request to a registration server that acts like a broker (e.g. one that is owned by a consortium of wireless service providers), which can in turn proxy the Radius Access-Request to the final home registration server. If the local registration server is unable to

service the registration request locally or by proxying, then it rejects the foreign agent's registration request and the foreign agent rejects the end system's registration request. Upon receiving the Radius Access-Request, the home registration server performs the necessary authentication of the identities of the foreign network and the end system. If authentication and registration succeeds, the home registration server responds with a Radius Access-Response packet to the foreign registration server which sends a response to the foreign agent so that a round trip can be completed. The registration request is rejected if the home registration server is unable to comply for any reason.

The second level of authentication verifies the identity of the end system to the intranet or ISP PPP server. PPP authentication, separate from mobility authentication allows the infrastructure equipment to be deployed and owned separately from the ISP.

FIG. 14 is a ladder diagram showing the registration sequence for a roaming end system. It is assumed that the PPP server and the home IWF are in the same server and L2TP is not required. Note the interactions with accounting servers to start accounting on behalf of the registering end system and also directory servers to determine the identity of the home registration server and to authenticate the end system's identity. More information on accounting, billing, roaming (between service providers) and settlement will be provided below.

MAC layer messages from the user registration agent of the end system may be used to initiate Agent Solicitation. The MAC layer messages are not shown for clarity.

In FIG. 14, the end system (mobile) initially solicits an advertisement and the foreign agent replies with an advertisement that provides the end system with information about the network to which the foreign agent belongs including a care-of-address of the foreign agent. Alternatively, this phase may be removed and all network advertisements may be done by a continuously emitted MAC layer beacon message. In this case, the network is assumed to be a foreign wireless service provider. Then, a user registration agent (in the end system) incorporates the

information about the foreign agent (including the user name and other security credentials) and its network into a request and sends the request to the foreign agent. The foreign agent, as a proxy registration agent, relays the request to the foreign registration server (i.e., the registration server for the foreign wireless service provider. Then, the foreign registration server, recognizing that it is not the home directory, accesses the foreign directory server with the FDD in the foreign wireless service provider to learn how to direct the registration request to the home registration server of the wireless service provider to which the end system belongs. The foreign registration server responds with the necessary forwarding information. Then, the foreign registration server encapsulates the end system's registration request in a Radius access request and relays the encapsulated request to the home registration server of the wireless service provider to which the end system belongs. The home registration server accesses the home directory server with the HDD of the home registration server to learn at least authentication information about the foreign service provider. Optionally, the home registration server accesses the subscriber's directory to learn detail subscriber service profile information (e.g., quality of service options subscribed to, etc.). When all parties are authenticated, the home registration server sends a start IWF request to the home IWF and PPP server. The home IWF and PPP server starts the home accounting server and then sends a start IWF response to the home registration server. The home registration server then sends a Radius access response to the foreign registration server. The foreign registration server then sends a start IWF request to the serving IWF server. The serving IWF server starts the serving accounting server and then sends a start IWF response to the foreign registration server. The foreign registration server sends a registration reply to the foreign agent, and the foreign agent relays the registration reply to the end system.

A link control protocol (LCP) configuration request is send by the end system through the foreign registration server to the home IWF and PPP server. The home IWF and PPP server sends an LCP configuration acknowledgment through the foreign registration server to the end system.

Similarly, a password authentication protocol (PAP) authentication request is sent to and acknowledged by the home IWF and PPP server. Alternatively, a challenge authentication protocol (CHAP) may be used to authenticate. Both protocols may be used to authenticate or this phase may be skipped.

Similarly, an IP configuration protocol (IPCP) configure request is sent to and acknowledged by the home IWF and PPP server.

The connection to the end system may be terminated because of any one of the following reasons.

1. *User initiated termination*. Under this scenario, the end system first terminates the PPP gracefully. This includes terminating the PPP network control protocol (IPCP) followed by terminating the PPP link protocol. Once this is done, the end system de-registers from the network followed by termination of the radio link to the access point.

2. *Loss of wireless link*. This scenario is detected by the modem and reported to the modem driver in the end system. The upper layers of the software are notified to terminate the stacks and notify the user.

3. *Loss of connection to the foreign agent*. This scenario is detected by the mobility driver in the end system. After trying to re-establish contact with a (potentially new) foreign agent and failing, the driver sends an appropriate notification up the protocol stack and also signals the modem hardware below to terminate the wireless link.

4. *Loss of connection to the IWF*. This is substantially the same as for loss of connection to the foreign agent.

5. *Termination of PPP by IWF or PPP server*. This scenario is detected by the PPP software in the end system. The end system's

PPP driver is notified of this event. It initiates de-registration from the network followed by termination of the wireless link to the access point.

End system service configuration refers to the concept of configuring the network service for an end system based on the subscriber's service profile. The subscriber's service profile is stored in a subscriber directory. The service profile contains information to enable the software to customize wireless data service on behalf of the subscriber. This includes information to authenticate the end system, allow the end system to roam and set up connections to the end system's internet service provider. Preferably, this information also includes other parameters, like, quality of service. In addition to the subscriber directory, a home domain directory (HDD) and a foreign domain directory (FDD) are used for roaming and for authenticating the foreign and home registration servers to each other. The HDD stores information about the end system's home network and the FDD stores information about foreign networks that a subscriber may visit.

FIG. 15 shows how these directories map into the network architecture and are used during registration for an end system that is registering at home. In step 0 the end system (mobile) solicits and receives an advertisement from the foreign agent to provides the end system with information about the network to which the foreign agent belongs. In this case, the network is the home wireless service provider. In step 1, user registration agent (in the end system) incorporates the information about the foreign agent and its network and its security credentials into a request and sends the request to the foreign agent. In step 2, the foreign agent, as a proxy registration agent, relays the request to the home registration server. In step 3, the home registration server accesses the HDD of the home wireless service provider to learn at least authentication information. In step 4, the home registration server accesses the subscriber directory to learn detail subscriber service profile information (e.g., quality of service options subscribed to, etc.). In step 5, the home registration server notifies the foreign agent of the access response. In steps 6 and 7, the foreign agent notifies the end system (i.e., mobile) of the registration reply.

FIG. 16 shows directory usage for an end system that is registering from a foreign network. In step 0 the end system (mobile) solicits and receives an advertisement and the foreign agent advertises which provides the end system with information about the network to which the foreign agent belongs. In this case, the network is a foreign wireless service provider. In step 1, user registration agent (in the end system) incorporates the information about the foreign agent and its network and its security credential into a request and sends the request to the foreign agent. In step 2, the foreign agent, as a proxy registration agent, relays the request to the foreign registration server (i.e., the registration server for the foreign wireless service provider. In step 3, the foreign registration server accesses the HDD of foreign wireless service provider to learn the network to which the end system belongs. In step 4, the foreign registration server forwards the end system's request to the home registration server of the end system's home wireless service provider. In step 5, the home registration server accesses the FDD of the home registration server to learn at least authentication information about the foreign service provider. In step 6, the home registration server accesses the subscriber's directory to learn detail subscriber service profile information (e.g., quality of service options subscribed to, etc.). In step 7, the home registration server notifies the foreign registration server of the access response. In step 8, the foreign registration server forwards to the foreign agent the access response. In step 9, the foreign agent notifies the end system (i.e., mobile) of the registration reply.

Protocol handling scenarios handle bearer data and the associated stacks for transporting bearer data to and from an end system. The protocol stacks for the cell architectures use local APs (FIG. 17) and remote APs (FIG. 18).

FIG. 17 shows the protocol stacks for handling communications between an end system (in its home network) and a home IWF for End System @ Home. FIG. 17 shows the protocol handling for a cell architecture where the access point and the wireless hub are co-located.

FIG. 18 shows the protocol handling for a cell architecture where the access point is located remotely from the wireless hub. As shown, PPP terminates in the IWF and the configuration provides direct internet access. The configuration for the case where the PPP server is separate from the IWF is described later.

In FIG. 18, PPP frames from the end system are encapsulated in RLP (radio link protocol) frames which are encapsulated at the remote access point in MAC frames for communicating with the trunk access point (i.e., an access point physically located near the wireless hub), the remote access point being coupled to the access point by, for example, a wireless trunk). The access point functions as a MAC layer bridge and relays frames from the air link to the foreign agent in the wireless hub. The foreign agent de-encapsulates the RLP frames out of the MAC frames, and using the *xtunnel* protocol, relays the RLP frames to the IWF. A similar, albeit reverse, process occurs for transmitting frames from the IWF to the end system.

If the end system moves to another foreign agent, then a new *xtunnel* will be automatically created between the new foreign agent and the IWF, so that PPP traffic continues to flow between them, without interruption.

In the remote AP cell architecture (FIG. 18) using wireless trunks between the remote AP and the trunk AP, the air link between the end system and the access point may operate at a different frequency (f1) and use a different radio technology as compared to the frequency (f2) and radio technology of the trunk.

FIG. 19 shows the protocol stacks for a roaming end system. The serving IWF uses of the *I-xtunnel* protocol between the serving IWF and home IWF. The rest of the protocol stacks remain unchanged and are not shown. This architecture may be simplified by merging the serving IWF into the base station, thus eliminating the XWD protocol.

The RLP layer uses sequence numbers to drop duplicate PPP datagrams and provide in-sequence delivery of PPP datagrams between the end system and

the IWF. It also provides a configurable keep-alive mechanism to monitor link connectivity between the end system and the IWF. Additionally, in an alternative embodiment, the RLP layer also provides re-transmission and flow control services in order to reduce the overall bit error rate of the link between the end system and the IWF. The RLP between the end system and the IWF is started at the beginning of the session and remains active throughout the session and even across hand-offs.

In contrast to the specification in the mobile IP RFC (RFC 2003), IP in IP encapsulation is not used for tunneling between the foreign agent and the home IWF. Instead a new tunneling protocol, implemented on top of UDP is used. This tunneling protocol is a simplified version of the L2TP protocol. The reasons for this choice are as follows.

1. The encapsulation protocol specified in RFC 2003 does not provide flow control or in-sequence delivery of packets. The presently described network may need these services in the tunnel over the backhaul. Flow control may be needed to reduce the amount of re-transmissions over the air link because of packet loss due to flow control problems over the network between the base station and the MSC or because of flow control problems in the base station or the IWF.

2. By using a UDP based tunneling protocol, the implementation can be done at the user level and then put into the kernel for performance reasons, after it has been debugged.

3. Using RFC 2003, there is no easy way of creating tunnels taking into account quality of service and load balancing. In order to take QOS into account, it should be possible to set up tunnels over links that already provide the required QOS. Secondly, using RFC 2003, there is no easy way to provide load balancing to distribute bearer traffic load over multiple links between the base station and the MSC.

4. In order to implement IP in IP encapsulation as specified in RFC 2003, developers require access to IP source code. In commercial operating systems, source code for the TCP/IP stack is generally proprietary to other equipment manufacturers. Purchasing the TCP/IP stack from a vendor and making changes to the IP layer to support mobile IP tunneling would require a developer to continue supporting a variant version of the TCP/IP stack. This adds cost and risk.

While it is noted that the tunneling protocol between the base station and the IWF is non-standard and that the wireless service provider will not be able to mix and match equipment from different vendors, the use of a non-standard tunneling protocol within a single wireless service provider network is transparent to end systems and equipment from other vendors.

The new tunneling protocol is based on L2TP. By itself, L2TP is a heavyweight tunneling protocol so that L2TP has a lot of overhead associated with tunnel creation and authentication. The new tunneling protocol of the present system has less overhead. The new xtunnel protocol has the following features.

1. The *xtunnel* creation adds vendor specific extensions to Radius Access Request and Radius Access Response messages between the base station and the registration server. These extensions negotiate tunnel parameters and to create the tunnel.

2. The registration server is able to delegate the actual work of tunneling and relaying packets to a different IP address, and therefore, to a different server in the MSC. This permits the registration server to do load balancing across multiple IWF servers and to provide different QOS to various users.

3. The *xtunnel* protocol supports in-band control messages for tunnel management. These messages include echo request/response to test tunnel connectivity, disconnect request/response/notify to

disconnect the tunnel and error notify for error notifications. These messages are sent over the tunneling media, for example, UDP/IP.

4. The *xtunnel* protocol sends payload data over the tunneling media, for example, UDP/IP. The *xtunnel* protocol supports flow control and in-sequence packet delivery.

5. The *xtunnel* protocol may be implemented over media other than UDP/IP for quality of service.

The network supports direct internet connectivity by terminating the PPP in the home IWF and routing IP packets from the IWF to the internet via a router using standard IP routing techniques. Preferably, the IWF runs Routing Information Process (RIP), and the router also runs RIP and possibly other routing protocols like Open Shortest Path First (OSPF).

The network supports a first configuration for a wireless service provider who is also an internet service provider. In this configuration, the home IWF in the MSC also functions as a PPP server. This IWF also runs internet routing protocols like RIP and uses a router to connect to the internet service provider's backbone network.

The network supports a second configuration for a wireless service provider who wishes to allow end systems to connect to one or more internet service providers, either because the WSP itself is not ISPs, or because the WSP has agreements with other ISPs to provide access to end users. For example, a wireless service provider may elect to offer network access to an end user and may have an agreement with a 3rd party ISP to allow the user who also has an account with the 3rd party ISP to access the ISP from the WSP network. In this configuration, the PPP server does not run in the home IWF installed at the MSC. Instead, a tunneling protocol like L2TP (Layer Two Tunneling Protocol) is used to tunnel back to the ISP's PPP server. FIG. 10 shows the protocol stacks for this configuration for an end system that is at home.

The location of the home IWF and the ISP PPP server remains fixed throughout the PPP session. Also, the L2TP tunnel between the IWF and the ISP's PPP server remains up throughout the PPP session. The physical link between the IWF and the PPP server is via a router using a dedicated T1 or T3 or frame relay or ATM network. The actual nature of the physical link is not important from the point of view of the architecture.

This configuration also supports intranet access. For intranet access, the PPP server resides in the corporate intranet and the home IWF uses L2TP to tunnel to it.

For a fixed end system, the protocol handling for intranet or ISP access is as shown in FIG. 20 with the difference that the roaming end system uses a serving IWF to connect to its home IWF. The protocol handling between a serving IWF and a home IWF has been described earlier. In Figure 20, the home IWF may be merged into the wireless hub eliminating the X-Tunnel protocol. Also, the serving IWF may be merged into the wireless hub, thus eliminating the X-Tunnel protocol.

FIG. 21 shows the protocol stacks used during the registration phase (end system registration) for a local AP cell architecture. The stack for a remote AP cell architecture is very similar.

The scenario shown above is for a roaming end system. For an end system at home, there is no foreign registration server in the registration path.

Note the mobility agent in the end system. The mobility agent in the end system and foreign agent in the wireless hub are conceptually similar to the mobile IP RFC 2002. The mobility agent handles network errors using time-outs and re-trys. Unlike the known protocol stacks for bearer data, RLP is not used. The foreign agent and the registration servers use Radius over UDP/IP to communicate with each other for registering the end system.

Several aspects of security must be considered. The first, authenticating the identities of the end system and the foreign/home networks during the wireless

registration phase. Second, authenticating the identity of the end system with its PPP server during the PPP authentication phase. Third, authentication for storing accounting data, for billing and for updating home domain information. Fourth, encryption of bearer traffic transmitted to and from the end system. Fifth, encryption for exchanging billing information across service provider boundaries.

Shared secrets are used to authenticate the identity of end systems with their home networks and the identity of the home and foreign networks with each other during wireless registration.

End system authentication uses a 128-bit shared secret to create an authenticator for its registration request. The authenticator is created using the known MD5 message digest algorithm as described in the mobile IP RFC 2002. Alternatively, a different algorithm may be used. The shared secret is not sent in the registration request by the end system. Only the authenticator is sent. On receiving the registration request from the end system, the home registration server re-computes the authenticator over the registration request data using the shared secret. If the computed authenticator value matches the authenticator value sent by the end system, the home registration server allows the registration process to proceed. If the values do not match, the home registration server logs the event, generates a security violation alarm and a nak (i.e., a negative acknowledgment) to the request.

In the registration reply, the home registration server does the same - that is to say, uses the shared secret to create an authenticator for the registration reply that it sends to the end system. Upon receiving the reply, the end system re-computes the authenticator using the shared secret. If the computed value does not match the authenticator value sent by the home registration server in the reply, the end system discards the reply and tries again.

These network security concepts are similar to the concepts defined in mobile IP RFC 2002. According to the RFC, a mobility security association exist between each end system and its home network. Each mobility security association defines a collection of security contexts. Each security context defines

an authentication algorithm, a mode, a secret (shared or public-private), style of replay protection and the type of encryption to use. In the context of the present network, the end system's User-Name (in lieu of the mobile IP home address) is used to identify the mobility security association between the end system and its home network. Another parameter, called the security parameter index (SPI), is used to select a security context within the mobility security association. In a basic embodiment of the invention, only the default mobile IP authentication algorithm (keyed-MD5) and the default mode ("prefix+suffix") are supported with 128-bit shared secrets. Network users are allowed to define multiple shared secrets with their home networks. The mechanism for creating security contexts for end users, assigning an SPI to each security context and for setting the contents of the security context (which includes the shared secret) and for modifying their contents are described below. During registration, a 128-bit message digest is computed by the end system in prefix+suffix mode using the MD5 algorithm. The shared secret is used as the prefix and the suffix for the data to be protected in the registration request. The authenticator thus computed, along with the SPI and the User-Name are transmitted in the registration request by the end system. Upon receiving the end system's registration request, the foreign registration server relays the request along with the authenticator and the SPI, unchanged to the home registration server. Upon receiving the registration request directly from the end system or indirectly via a foreign registration server, the home registration server uses the SPI and the User-Name to select the security context. The home server re-computes the authenticator using the shared secret. If the computed authenticator value matches the value of the authenticator sent in the request by the end system, the user's identity will have been successfully authenticated. Otherwise, the home registration server naks (negatively acknowledges) the registration request sent by the end system.

The registration reply sent by the home registration server to the end system is also authenticated using the algorithm described above. The SPI and the computed authenticator value is transmitted in the registration reply message by the home server to the end system. Upon receiving the reply, the end system re-

computes the authenticator, and if the computed value does not match the transmitted value, it will discard the reply and retry.

The user's end system has to be configured with the shared secret and SPIs for all security contexts that the user shares with its registration server(s). This configuration information is preferably stored in a Win 95 registry for Windows 95 based end systems. During registration, this information is accessed and used for authentication purposes.

In the network, Radius protocols are used by foreign agent FA to register the end system and to configure the *xtunnel* between the wireless hub and the home and serving IWFs on behalf of the end system. On receiving a registration request from the end system, the FA creates a Radius Access-Request packet, stores its own attributes into the packet, copies the end system's registration request attributes unchanged into this packet and sends the combined request to the registration server in the MSC.

Radius authentication requires that the Radius client (in this case, the FA in the base station) and the Radius server (in this case, the registration server in the MSC) share a secret for authentication purposes. This shared secret is also used to encrypt any private information communicated between the Radius client and the Radius server. The shared secret is a configurable parameter. The network follows the recommendations in the Radius RFC and uses the shared secret and the MD5 algorithm for authentication and for encryption, where encryption is needed. The Radius-Access Request packet sent by the FA contains a Radius User-Name attribute (which is provided by the end system) and a Radius User-Password attribute. The value of the User-Password attribute is also a configurable value and encrypted in the way recommended by the Radius protocol. Other network specific attributes, which are non-standard attributes from the point of view of the Radius RFC standards, are encoded as vendor specific Radius attributes and sent in the Access-Request packet.

The following attributes are sent by the FA to its registration server in the Radius Access-Request packet.

1. *User-Name Attribute.* This is the end system's user-name as supplied by the end system in its registration request.

2. *User-Password Attribute.* This user password is supplied by the base station/wireless hub on behalf of the user. It is encoded as described in the Radius EFC using the secret shared between the base station and its registration server.

3. *NAS-Port.* This is the port on the base station.

4. *NAS-IP-Address.* This is the IP address of the base station.

5. *Service-Type.* This is framed service.

6. *Framed Protocol.* This is a PPP protocol.

7. *Xtunnel Protocol Parameters.* These parameters are sent by the base station to specify the parameters necessary to set up the *xtunnel* protocol on behalf of the end system. This is a vendor-specific attribute.

8. *AP-IP-Address.* This is the IP address of the AP through which the user is registering. This is a vendor-specific attribute.

9. *AP-MAC-Address.* This is the MAC address of the AP through 10.

10. *End system's Registration Request.* The registration request from the end system is copied unchanged into this vendor specific attribute.

The following attributes are sent to the FA from the registration server in the Radius Access-Response packet.

1. *Service Type.* This is a framed service.

2. *Framed-Protocol.* This is a PPP.

3. 3. *Xtunnel Protocol Parameters*. These parameters are sent by the registration server to specify the parameters necessary to set up the *xtunnel* protocol on behalf of the end system. This is a vendor-specific attribute.

4. *Home Registration Server's Registration Reply*. This attribute is sent to the FA from the home registration server. The FA relays this attribute unchanged to the end system in a registration reply packet. If there is a foreign registration server in the path, this attribute is relayed by it to the FA unchanged. It is coded as a vendor-specific attribute.

To provide service to roaming end systems, the foreign network and the home network are authenticated to each other for accounting and billing purposes using the Radius protocol for authentication and configuration. This authentication is performed at the time of end system registration. As described earlier, when the registration server in the foreign network receives a registration request from an end system (encapsulated as a vendor specific attribute in a Radius-Access Request packet by the FA), it uses the end system's User-Name to determine the identity of the end system's home registration server by consulting its home domain directory HDD. The following information is stored in home domain directory HDD and accessed by the foreign registration server in order to forward the end system's registration request.

1. *Home Registration Server IP Address*. This is the IP address of the home registration server to forward the registration request.

2. *Foreign Registration Server Machine Id*. This is the machine ID of the foreign registration server in SMTP (simplified mail transfer protocol) format (e.g., machine@fqdn where machine is the name of the foreign registration server machine and fqdn is the fully qualified domain name of the foreign registration server's domain).

3. *Tunneling Protocol Parameters*. These are parameters for configuring the tunnel between the serving IWF and the home IWF on behalf of the end system. These include the tunneling protocol to be used between them and the parameters for configuring the tunnel.

4. *Shared Secret*. This is the shared secret to be used for uthentication between the foreign registration server and the home registration server. This secret is used for computing the Radius User-Password attribute in the Radius packet sent by the foreign registration server to the home registration server. It is defined between the two wireless service providers.

5. *User-Password*. This is the user password to be used on behalf of the roaming end system. This user password is defined between the two wireless service providers. This password is encrypted using the shared secret as described in the Radius RFC.

6. *Accounting Parameters*. These are parameters for configuring accounting on behalf of the end system that is registering. These parameters are sent by the registration server to its IWF for configuring accounting on behalf of the end system.

Using this information, the foreign registration server creates a Radius Access-Request, adds its own registration and authentication information into the Radius Access-Request, copies the registration information sent by the end system unchanged into the Radius Access-Request and sends the combined request to the home registration server.

Upon receiving the Radius-Access Request from the foreign registration server (for a roaming end system) or directly from the FA (for an end system at home), the home registration server consults its own directory server for the shared secrets to verify the identity of the end system and the identity of the foreign registration server in a roaming scenario by re-computing authenticators.

After processing the request successfully, the home registration server creates a Radius Access-Accept response packet and sends it to the foreign registration server if the end system is roaming, or directly to the FA from which it received the Radius Access-Request. The response contains the registration reply attribute that the FA relays to the end system.

If the request can not be processed successfully, the home registration server creates a Radius Access-Reject response packet and sends it to the foreign registration server if the end system is roaming, or directly to the FA from which it received the Radius Access-Request. The response contains the registration reply attribute that the FA will relays to the end system.

In a roaming scenario, the response from the home registration server is received by the foreign registration server. It is authenticated by the foreign registration server using the shared secret. After authenticating, the foreign registration server processes the response, and in turn, it generates a Radius response packet (Accept or Reject) to send to the FA. The foreign registration server copies the registration reply attribute from the home registration server=s Radius response packet, unchanged, into its Radius response packet.

When the FA receives the Radius Access-Response or Radius Access-Reject response packet, it creates a registration reply packet using the registration reply attributes from the Radius response, and sends the reply to the end system, thus completing the round trip registration sequence.

Mobile IP standards specifies that replay protection for registrations are implemented using time stamps, or optionally, using nonces. However, since replay protection using time stamps requires adequately synchronized time-of-day clocks between the corresponding nodes, the present system implements replay protection during registration using nonces even though replay protection using time stamps is mandatory in the Mobile IP standards and the use nonces is optional. However, replay protection using time stamps as an alternative embodiment is envisioned.

The style of replay protection used between nodes is stored in the security context in addition to the authentication context, mode, secret and type of encryption.

The network supports the use of PPP PAP (password authentication) and CHAP (challenge authenticated password) between the end system and its PPP server. This is done independently of the registration and authentication mechanisms described earlier. This allows a private intranet or an ISP to independently verify the identity of the user.

Authentication for accounting and directory services is described below with respect to accounting security. Access to directory servers from network equipment in the same MSC need not be authenticated.

The network supports encryption of bearer data sent between the end system and the home IWF. End systems negotiate encryption to be on or off by selecting the appropriate security context. Upon receiving the registration request, the home registration server grants the end system's request for encryption based upon the security context. In addition to storing the authentication algorithm, mode, shared secret and style of replay protection, the security context is also used to specify the style of encryption algorithm to use. If encryption is negotiated between the end system and the home agent, then the complete PPP frame is so encrypted before encapsulation in RLP.

The IWF, the accounting server and the billing system are part of the same trusted domain in the MSC. These entities are either connected on the same LAN or part of a trusted intranet owned and operated by the wireless service provider. Transfer of accounting statistics between the IWF and the accounting server and between the accounting server and the customer's billing system may be encrypted using Internet IP security protocols like IP-Sec.

The network makes it more difficult to monitor the location of the end system because it appears that all PPP frames going to and from the end system go through the home IWF regardless of the actual location of the end system device.

Accounting data is collected by the serving IWF and the home IWF in the network. Accounting data collected by the serving IWF is sent to an accounting server in the serving IWF's MSC. Accounting data collected by the home IWF is sent to an accounting server in the home IWF's MSC. The accounting data collected by the serving IWF is used by the foreign wireless service provider for auditing and for settlement of bills across wireless service provider boundaries (to support roaming and mobility). The accounting data collected by the home IWF is used for billing the end user and also for settlement across wireless service provider boundaries to handle roaming and mobility.

Since all data traffic flows through the home IWF, regardless of the end system's location and the foreign agent's location, the home IWF has all the information to generate bills for the customer and also settlement information for the use of foreign networks.

The serving IWF and the home IWF preferably use the Radius accounting protocol for sending accounting records for registered end systems. The Radius accounting protocol is as documented in a draft IETF RFC. For the present invention, the protocol has to be extended by adding vendor specific attributes for the network and by adding check-pointing to the Radius Accounting protocol. Check-pointing in this context refers to the periodic updating of accounting data to minimize risk of loss of accounting records.

The Radius accounting protocol runs over UDP/IP and uses re-trys based on acknowledgment and time outs. The Radius accounting client (serving IWFs or home IWFs) send UDP accounting request packets to their accounting servers which send acknowledgments back to the accounting clients.

In the network, the accounting clients (serving IWF and the home IWF) emit an accounting start indication at the start of the user's session and an accounting stop indication at the end of the user's session. In the middle of the session, the accounting clients emit accounting checkpoint indications. In contrast, the Radius accounting RFC does not specify an accounting checkpoint indication. The software of the present system creates a vendor specific accounting attribute

for this purpose. This accounting attribute is present in all Radius Accounting-Request packets which have Acct-Status-Type of Start (accounting start indications). The value of this attribute is used to convey to the accounting server whether the accounting record is a check-pointing record or not. Check-pointing accounting reports have a time attribute and contain cumulative accounting data from the start of the session. The frequency of transmitting check-point packets is configurable in the present invention.

The serving IWF and the home IWF are configured by their respective registration servers for connecting to their accounting servers during the registration phase. The configurable accounting parameters include the IP address and UDP port of the accounting server, the frequency of check-pointing, the session/multi-session id and the shared secret to be used between the accounting client and the accounting server.

The network records the following accounting attributes for each registered end system. These accounting attributes are reported in Radius accounting packets at the start of the session, at the end of the session and in the middle (check-point) by accounting clients to their accounting servers.

1. *User Name*. This is like the Radius User-Name attribute discussed above. This attribute is used to identify the user and is present in all accounting reports. The format is "user@domain" where domain is the fully qualified domain name of the user's home.

2. *NAS IP Address*. This is like the Radius NAS-IP-Address attribute discussed above. This attribute is used to identify the IP address of the machine running the home IWF or the serving IWF.

3. *Radio Port*. This attribute identifies the radio port on the access point providing service to the user. This attribute is encoded as a vendor specific attribute.

4. *Access Point IP Address*. This attribute identifies the IP address of the access point providing service to the user. This attribute is encoded as a vendor specific attribute.

5. *Service Type*. This is like the Radius Service-Type attribute described above. The value of this attribute is Framed.

6. *Framed Protocol*. This is like the Radius Framed-Protocol attribute described above. The value of this attribute is set to indicate PPP.

7. *Accounting Status Type*. This is like the Radius Acct-Status-Type attribute described above. The value of this attribute may be Start to mark the start of a user's session with the Radius client and Stop to mark the end of the user's session with the Radius client. For accounting clients, the Acct-Status-Type/Start attribute is generated when the end system registers. The Acct-Status-type/Stop attribute is generated when the end system de-registers for any reason. For checkpoints, the value of this attribute is also Start and the *Accounting Checkpoint* attribute is also present.

8. *Accounting Session Id*. This is like the Radius Acct-Session-Id described above. In a roaming scenario, this session id is assigned by the foreign registration server when the end system issues a registration request. It is communicated to the home registration server by the foreign registration server during the registration sequence. The home network and the foreign network both know the Acct-Session-Id attribute and are able to emit this attribute while sending accounting records to their respective accounting servers. In a "end system-at-home" scenario, this attribute is generated by the home registration server. The registration server communicates the value of this attribute to the IWF which emits it in all accounting records.

9. *Accounting Multi-Session Id.* This is like the Radius Acct-Multi-Session-Id discussed above. This id is assigned by the home registration server when a registration request is received from a FA directly or via a foreign registration server on behalf of an end system. It is communicated to the foreign registration server by the home registration server in the registration reply message. The registration server(s) communicates the value of this attribute to the IWF(s) which emit it in all accounting records.

With true mobility added to the architecture, the id is used to relate together the accounting records from different IWFs for the same end system if the end system moves from one IWF to another. For hand-offs across IWF boundaries, the Acct-Session-Id is different for accounting records emanating from different IWFs. However, the Acct-Multi-Session-Id attribute is the same for accounting records emitted by all IWFs that have provided service to the user. Since the session id and the multi-session id are known to both the foreign network and the home network, they are able to emit these attributes in accounting reports to their respective accounting servers. With the session id and the multi-session id, billing systems are able to correlate accounting records across IWF boundaries in the same wireless service provider and even across wireless service provider boundaries.

1. *Accounting Delay Time.* See Radius Acct-Delay-Time attribute.

2. *Accounting Input Octets.* See Radius Acct-Input-Octets. This attribute is used to keep track of the number of octets sent by the end system (input to the network from the end system). This count is used to track the PPP frames only. The air link overhead, or any overhead imposed by RLP, etc. is not counted.

3. *Accounting Output Octets.* See Radius Acct-Output-Octets. This attribute is used to keep track of the number of octets sent to the end system (output from the network to the end system). This

count is used to track the PPP frames only. The air link overhead, or any overhead imposed by RLP, etc. and is not counted.

4. *Accounting Authentic*. See Radius Acct-Authentic attribute. The value of this attribute is Local or Remote depending on whether the serving IWF or the home IWF generates the accounting record.

5. *Accounting Session Time*. See Radius Acct-Session-Time attribute. This attribute indicates the amount of time that the user has been receiving service. If sent by the serving IWF, this attribute tracks the amount of time that the user has been receiving service from that serving IWF. If sent by the home IWF, this attribute tracks the amount of time that the user has been receiving service from the home IWF.

6. *Accounting Input Packets*. See Radius Acct-Input-Packets attribute. This attribute indicates the number of packets received from the end system. For a serving IWF, this attribute tracks the number of PPP frames input into the serving IWF from an end system. For a home IWF, this attribute tracks the number of PPP frames input into the home IWF from an end system.

7. *Accounting Output Packets*. See Radius Acct-Output-Packets attribute. This attribute indicates the number of packets sent to the end system. For a serving IWF, this attribute tracks the number of PPP frames output by the serving IWF to the end system. For a home IWF, this attribute tracks the number of PPP frames sent to the end system from the home IWF.

8. *Accounting Terminate Cause*. See Radius Acct-Terminate-Cause attribute. This attribute indicates the reason why a user session was terminated. In addition, a specific cause code is also present to

provide additional details. This attribute is only present in accounting reports at the end of the session.

9. *Network Accounting Terminate Cause*. This attribute indicates a detailed reason for terminating a session. This specific attribute is encoded as a vendor specific attribute and is only reported in a Radius Accounting attribute at the end of session. The standard Radius attribute Acct-Terminate-Cause is also present. This attribute provides specific cause codes, not covered by the Acct-Terminate-Cause attribute.

10. *Network Air link Access Protocol*. This attribute indicates the air link access protocol used by the end system. This attribute is encoded as a vendor specific attribute.

11. *Network Backhaul Access Protocol*. This attribute indicates the backhaul access protocol used by the access point to ferry data to and from the end system. This attribute is encoded as a vendor specific attribute.

12. *Network Agent Machine Name*. This attribute is the fully qualified domain name of the machine running the home IWF or the serving IWF. This specific attribute is encoded in vendor specific format.

13. *Network Accounting Check-point*. Since the Radius accounting RFC does not define a check-point packet, the present network embodiment uses a Radius accounting start packet with this attribute to mark a check-point. The absence of a check-point attribute means a conventional accounting start packet. The presence of this attribute in a accounting start packet means a accounting check-point packet. Accounting stop packets do not have this attribute.

In the preferred embodiment, every accounting packet and the corresponding reply must be authenticated using MD5 and a shared secret. The IWFs are configured with a shared secret that are used by them for authentication

during communication with their Radius accounting server. The shared secrets used by the IWFs for communicating with accounting servers are stored in the home/foreign domain directory located in the MSC. The shared secrets for accounting security are communicated to the IWFs by their registration servers during the end system registration sequence.

The accounting server software runs in a computer located in the MSC. The role of the accounting server in the system is to collect raw accounting data from the network elements (the home and the serving IWFs), process the data and store it for transfer to the wireless service provider's billing system. The accounting server does not include a billing system. Instead, it includes support for an automatic or manual accounting data transfer mechanism. Using the automatic accounting data transfer mechanism, the accounting server transfers accounting records in AMA billing format to the customer's billing system over a TCP/IP transport. For this purpose, the system defines AMA billing record formats for packet data. Using the manual transfer mechanism, customers are able to build a tape to transfer accounting records to their billing system. In order to build the tape to their specifications, customers are provided with information to access accounting records so that they may process them before writing them to tape.

In FIG. 22, the raw accounting data received by the accounting server from the home or serving IWFs are processed and stored by the accounting server. The processing done by the accounting server includes filtering, compression and correlation of the raw accounting data received from the IWF. A high availability file server using dual active/standby processors and hot swappable RAID disks is used for buffering the accounting data while it is transiting through the accounting server.

The accounting server delays processing of the raw accounting data until an end system has terminated its session. When an end system terminates its session, the accounting server processes the raw accounting data that it has collected for the session and stores an accounting summary record in a SQL database. The

accounting summary record stored in the SQL data base points to an ASN.1 encoded file. This file contains detailed accounting information about the end system's session. The data stored in the accounting server is then transferred by the billing data transfer agent to the customer's billing system. Alternatively, the wireless service provider may transfer the accounting data from the SQL database and/or the ASN.1 encoded file to the billing system via a tape. The data base scheme and the format of the ASN.1 encoded file are documented and made available to customers for this purpose. If the volume of processed accounting data stored in the accounting system exceeds a high water mark, the accounting server generates an NMS alarm. This alarm is cleared when the volume of data stored in the accounting server falls below a low water mark. The high and low water marks for generating and clearing the alarm are configurable. The accounting server also generates an NMS alarm if the age of the stored accounting data exceeds a configurable threshold. Conversely, the alarm is cleared, when the age of the accounting data falls below the threshold.

The subscriber directory is used to store information about subscribers and is located in the home network. The home registration server consults this directory during the registration phase to authenticate and register an end system. For each subscriber, the subscriber directory stores the following information.

1. *User-Name*. This field in the subscriber record will be in SMTP format (e.g., *user@fqdn)* where the *user* sub-field will identify the subscriber in his or her wireless home domain and the *fqdn* sub-field will identify the wireless home domain of the subscriber. This field is sent by the end system in its registration request during the registration phase. This field is assigned by the wireless service provider to the subscriber at the time of subscription to the network service. This field is different than the user name field used in PPP.

2. *Mobility Security Association*. This field in the subscriber record contains the mobility security association between the subscriber

and his or her home network. As described above, a mobility security association exists between each subscriber and its home registration server. The mobility security association defines a collection of security contexts. Each security context defines an authentication algorithm, an authentication mode, a shared secret, style of replay protection and the type of encryption (including no encryption) to use between the end system and its home server. During registration, the home registration server retrieves information about the subscriber's security context from the subscriber directory using the *User-Name* and the *security parameter index (SPI)* supplied by the end system in its registration request. The information in the security context is used for enforcing authentication, encryption and replay protection during the session. The mobility security association is created by the wireless service provider at the time of subscription. It is up to the wireless service provider to permit the subscriber to modify this association either by calling up a customer service representative or by letting subscribers access to a secure Web site. The Web site software will export web pages which the wireless service provider may make accessible to subscribers from a secure web server. In this way, subscribers are able to view/modify the contents of the mobility security association in addition to other subscriber information that the service provider may make accessible.

Modem MAC Address. This field contains the MAC address of the modem owned by the subscriber. In addition to the shared secret, this field is used during registration to authenticate the user. It is possible to turn off MAC address based authentication on a per user basis. The MAC address is communicated to the home registration server during registration.

4. *Enable MAC Address Authentication.* This field is used to determine if MAC address based authentication is *enabled* or *disabled*. If *enabled*, the home registration server checks the MAC address of the registering end system against this field to validate the end system's identity. If *disabled*, then no checking is done.

5. *Roaming Enabled Flag.* If this field is set to *enabled*, then the end system is allowed to roam to foreign networks. If this field is *disabled*, then the end system is not permitted to roam to foreign networks.

6. *Roaming Domain List.* This field is meaningful only if the *Roaming Enabled Flag* is set to *enabled*. This field contains a list of foreign domains that the end system is allowed to roam to. When the contents of this list is null and the *Roaming Enabled Flag* is set to *enabled*, the end system is allowed to roam freely.

7. *Service Enable/Disable Flag.* This field may be set to *disabled* by the system administrator to disable service to a subscriber. If this field is disabled, then the subscriber is permitted to register for service. If the subscriber is registered and the value of this field is set to disabled, then the subscriber's end system is immediately disconnected by the network.

8. *Internet Service Provider Association.* This field contains information about the subscriber's internet service provider. This information is used by the IWF during the PPP registration phase to perform authentication with the internet service provider on behalf of the end system and also to create a L2TP tunnel between the IWF and the internet service provider's PPP server. This field contains the identity of the subscriber's ISP. The IWF uses this information to access the ISP directory for performing authentication and setting up the L2TP tunnel on behalf of the end system.

9. *Subscriber's Name & Address Information.* This field contains the subscriber's name, address, phone, fax, e-mail address, etc.

The home domain directory (HDD) is used by the registration server to retrieve parameters about the end system to complete registration on behalf of the end system. Using this information, the registration server determines if the end system is registering at home or if the end system is a roaming end system. In the former case, the registration server assumes the role of a home registration server and proceed with end system registration. In the latter case, the registration server assumes the role of a foreign registration server and, acting as a Radius proxy, it forwards the request to the real home registration server whose identity it gets from this directory. For roaming end system, the parameters stored in the HDD include the IP address of the home registration server, the home-foreign shared secret, the home-serving IWF tunnel configuration etc. The HDD is located in the MSC.

The following information is stored in the HDD.

1. *Home Domain Name.* This field is used as the key to search the HDD for an entry that matches the fully qualified home domain name provided by the end system in its registration request.

2. *Proxy Registration Request.* This field is used by the registration server to determine if it should act as a foreign registration server and proxy the end system's registration request to the real home registration server.

3. *Home Registration Server DNS Name.* If the *proxy registration request* flag is TRUE, this field is used to access the DNS name of the real home registration server. Otherwise, this field is ignored. The DNS name is translated to an IP address by the foreign registration server. The foreign registration server uses the IP address to relay the end system's registration request.

4. *Foreign Domain Name.* If the *proxy registration request* flag is TRUE, this field is used to identify the foreign domain name to the end system's home registration server. Otherwise, this field is ignored. The foreign registration server uses this information to create the foreign server machine id in SMTP format, for example, *machine@fqdn*. This machine id is sent to the home registration server by the foreign registration server in the Radius-Access Request.

5. *Shared Secret.* If the *proxy registration request* flag is TRUE, the shared secret is used between the foreign and home registration servers to authenticate their identity with each other. Otherwise this field is ignored.

6. *Tunneling Protocol Parameters.* This field is used to store parameters to configure the tunnels to provide service to the end system. For an end system at home, this includes information on tunnel parameters between the base station and the home IWF and from the home IWF to the PPP server. For a roaming end system, this includes tunneling parameters from the base station to the serving IWF and from the serving IWF to the home IWF. At a minimum, for each tunnel, this field contains the type of tunneling protocol to use and any tunneling protocol specific parameters. For example, this field may contain the identifier for the tunneling protocol L2TP and any additional parameters required to configure the L2TP tunnel between the IWF and its peer.

7. *Accounting Server Association.* This field is used to store information needed by the IWF to generate accounting data on behalf of the end system. It contains the name of the accounting protocol (e.g. RADIUS), the DNS name of the accounting server and additional parameters specific to the accounting protocol like the UDP port number, the shared secret that the IWF must use in

the Radius Accounting protocol, the frequency of check-pointing, the seed for creating the session/multi-session id, etc. The accounting server's DNS name is translated to the accounting server's IP address, which is sent to the IWF.

For wireless service providers that have roaming agreements with each other, the HDD is used for authentication and to complete the registration process. If an end system roams from its home network to a foreign network, the foreign registration server in that network consults the HDD in its MSC to get information about the visiting end system's home registration and to authenticate the home network before it provides service to the visiting end system.

The software for home domain directory management preferably provides a graphical user interface (GUI) based HDD management interface for system administrators. Using this GUI, system administrators are able to view and update entries in the HDD. This GUI is not intended for use by foreign wireless network service providers to perform remote updates based on roaming agreements. It is only intended for use by trusted personnel of the home wireless service provider operating behind fire walls.

The foreign domain directory (FDD) provides functionality that is the reverse of the home domain directory. The FDD is used by the home registration server to retrieve parameters about the foreign registration server and the foreign network in order to authenticate the foreign network and create a tunnel between a serving IWF and a home IWF. These parameters include the home-foreign shared secret, the home IWF-serving IWF tunnel configuration, etc. The FDD is preferably located in the home registration server's MSC. The FDD is used by home registration servers for registering roaming end systems.

The following information will be stored in the FDD.

1. *Foreign Domain Name*. This field is used as the key to search the FDD for an entry that matches the fully qualified domain name of the foreign registration server relaying the registration request.

2. *Shared Secret.* This is the shared secret used between the foreign and home registration servers to authenticate their identity mutually with each other.

3. *Home IWF-Serving IWF Tunneling Protocol Parameters.* This field is used to store parameters to configure the tunnel between the home IWF and the serving IWF. At a minimum, this field contains the type of tunneling protocol to use and any tunneling protocol specific parameters. For example, this field may contain the identifier for the tunneling protocol L2TP and any additional parameters required to configure the L2TP tunnel between the serving IWF and the home IWF.

4. *Accounting Server Association.* This field is used to store information needed by the home IWF to generate accounting data on behalf of the end system. It contains the name of the accounting protocol (e.g. RADIUS), the DNS name of the accounting server and additional parameters specific to the accounting protocol like the UDP port number, the shared secret that the IWF must use in the Radius Accounting protocol, the frequency of check-pointing, the seed for creating the session/multi-session id, etc. The accounting server's DNS name is translated to the accounting server's IP address, which is sent to the foreign agent.

For wireless service providers that have roaming agreements with each other, the FDD is used to do authentication and complete the registration process. If an end system roams from its home network to a foreign network, the registration server in the home network consults the FDD in its MSC to get information and authenticate the foreign network providing service to the end system.

The foreign domain directory management software provides a graphical user interface (GUI) based FDD management interface for system administrators. Using this GUI, system administrators are able to view and update entries in the FDD. This GUI is not intended for use by foreign wireless network service providers to perform

remote updates based on roaming agreements. It is only intended for use by trusted personnel of the home wireless service provider operating behind firewalls.

The internet service provider directory (ISPD) is used by the home IWF to manage connectivity with ISPs that have service agreements with the wireless service provider so that subscribers may access their ISPs using the network. For each subscriber, the subscriber directory has an entry for the subscriber's ISP. This field points to an entry in the ISPD. The home IWF uses this information to set up the connection to the ISP on behalf of the subscriber.

The network architecture supports roaming. In order for roaming to work between wireless service providers, the architecture must support the setting up of roaming agreements between wireless service providers. This implies two things: (1) updating system directories across wireless service providers and (2) settlement of bills between service providers.

In order to allow subscribers access to internet service providers, the architecture supports roaming agreements with internet service providers. This implies that the architecture must be able to send data to and receive data from ISP PPP servers (i.e., that support industry standard protocols like PPP, L2TP and Radius). It also implies that the architecture handles directory updates for ISP access and settlement of bills with ISPs.

When roaming agreements are established between two wireless service providers, both providers have to update their home and foreign domain directories in order to support authentication and registration functions for end systems visiting their networks from the other network. At a minimum, the architecture of the present embodiment supports manual directory updates. When a roaming agreement is established between two wireless service providers, then the two parties to the agreement exchange information for populating their home and foreign domain directories. The actual updates of the directories is done manually by the personnel of the respective service providers. If later, the information in the home and foreign domain directories needs to be updated, the two parties to the agreement exchange the updated information and then manually apply their updates to the directories.

In an alternative embodiment, the directory management software incorporates developing standards in the IETF to enable roaming between internet service providers and to enable ISPs to automatically manage and discover roaming relationships. This makes manual directory management no longer necessary. The network system automatically propagates roaming relationships, and discovers them, to authenticate and register visiting end systems.

At a minimum, the network architecture just processes and stores the accounting data and makes the data available to the wireless service provider's billing system. It is up to the billing system to handle settlement of bills for roaming.

In an alternative embodiment, developing standards in the IETF to handle distribution of accounting records between internet service providers are incorporated into the network architecture to enable ISPs to do billing settlement for roaming end systems.

The system software supports access to ISPs and private intranets by supporting L2TP between the home IWF and the ISPs or intranet PPP server. The internet service provider directory contains information useful to the IWF for creating these tunnels. As access agreements between the wireless service provider and internet service providers are put in place, this directory is updated manually by the wireless service provider's personnel. Automatic updates and discovery of access relationships between the wireless service provider and internet service providers are presently contemplated and implemented as the internet standards evolve. While accessing an internet service provider, the subscriber receives two bills - one from the wireless service provider for the use of the wireless network and the second from the internet service provider. Although common billing that combines both types of charges is not handled by the minimum embodiment software, it is contemplated that the software will take advantage of internet standards for billing settlement as they evolve so that subscribers may receive a common bill based on roaming agreements between the ISP and wireless service providers.

The system includes a element management system for managing the network elements. From the element manager, system administrators perform configuration,

performance and fault/alarm management functions. The element management applications run on top of a web browser. Using a web browser, system administrators manage the network from anywhere that they have TCP/IP access. The element manager also performs an agent role for a higher level manager. In this role it exports an SNMP MIB for alarm and fault monitoring.

A higher level SNMP manager is notified of alarm conditions via SNMP traps. The higher level SNMP manager periodically polls the element manager's MIB for the health and status of the network. System management personnel at the higher level manager are able to view an icon representation of the network and its current alarm state. By pointing and clicking on the network element icon, systems management personnel execute element management applications using a web browser and perform more detailed management functions.

Inside the network, management of the physical and logical network elements is performed using a combination of the SNMP protocol and internal management application programming interfaces. Applications in the element manager use SNMP or other management APIs to perform network management functions.

Architecturally, the element management system includes two distinct sets of functional elements. The first set of functional elements, including the configuration data server, performance data monitor and health/status monitor and network element recovery software, executes on an HA server equipped with RAID disks. The second set of functional elements, including the management applications, executes on a dedicated, non-HA management system. Even if the element manager system becomes non-operational, the network elements continue to be able to run and report alarms and even be able to recover from fault conditions. However, since all the management applications execute in the non-HA element manager, if the element manager goes down, then recovery actions requiring human intervention are not possible until the element manager becomes operational.

The wireless hubs (WHs) in the base stations are typically owned by a wireless service provider (WSP), and they are connected to the WSP's registration server (RS) either via point-to-point links, intranets or the Internet. The WSP's registration server

is typically a software module executing on a processor to perform certain registration functions. Inter-working function units (IWF units) are typically software modules executing on a processor to perform certain interfacing functions. IWF units are typically connected to the registration servers via intranets/WAN, and the IWF units are typically owned by the WSP. However, the IWF units need not be located within the same LAN as the registration servers. Typically, accounting and directory servers (also software modules executing on a processor) are connected to the registration servers via a LAN in the service provider's Data Center (e.g., a center including one or more processors that hosts various servers and other software modules). Traffic from the end system is then routed via a router (connected to the LAN) to the public Internet or to an ISP=s intranet. The registration server located in a foreign WSP's network is referred to as the foreign registration server (FRS), and the registration server located in the end system's home network (where the mobile purchases its service) is referred to as the home registration server (HRS). The inter-working function unit in the home network is referred to as the home IWF while the inter-working function unit in the foreign network (i.e., the network the end system is visiting) is referred to as the serving IWF.

For fixed wireless service (i.e., a non-moving end system), an end system may register for service on the home network from the home network (e.g., at home service) or from a foreign network (e.g., roaming service). The end system receives an advertisement sent by an agent (e.g., an agent function implemented in software) in the wireless hub via the access point. There are both MAC-layer registration as well as network-layer registration to be accomplished. These may be combined together for efficiency.

For end systems at home (FIG. 23), the network layer registration (like a local registration) make's known to the home registration server the wireless hub to which the end system is currently attached. An IWF in the end system's home network will become the anchor or home IWF. Thus, PPP frames to and from the end system travel via the wireless hub to the home IWF in the home network. If the end system is at home, the home IWF is connected to the wireless hub via an XTunnel protocol.

For roaming wireless service (FIG. 24), the foreign registration server determines the identity of the home network of the roaming end system during the registration phase. Using this information, the foreign registration server communicates with the home registration server to authenticate and register the end system. The foreign registration server then assigns a serving IWF, and an I-XTunnel protocol connection is established between the home IWF and the serving IWF for the roaming end system. The serving IWF relays frames between the wireless hub and the home IWF. From the home IWF, data is sent to a PPP server (i.e., point-to-point protocol server) which may reside in the same IWF. However, if the data is to go to a corporate intranet or an ISP's intranet that has its own PPP server, the data is sent to the separate PPP server via the L2TP protocol. The separate server is typically owned and operated by an Internet service provider who is different from the wireless service provider. For the duration of the session, the locations of the home IWF and PPP server remain fixed. The MAC layer registration can be combined with the network registration to economize on the overhead of separate communications for MAC layer and network layer registration; however, it may be advantageous to not combine these registration processes so that the WSP's equipment will be interoperable with other wireless networks that supports pure IETF Mobile-IP.

Registration sets up three tables. Table 1 is associated with each access point, and Table 1 identifies each connection (e.g., each end system) by a connection id (CID) and associates the connection id with a particular wireless (WM) modem address (i.e., the address of the end system or end system). Table 2 is associated with each wireless hub (WH), and Table 2 associates each connection id with a corresponding wireless modem address, access point and XTunnel id (XID). Table 3 is associated with each inter-working function (IWF), and Table 3 associates each connection id with a corresponding wireless modem address, wireless hub address, XTunnel id and IP port (IP/port). The entries described for these tables are described to include only relevant entries that support the discussion of mobility management. In reality, there are other important fields that need to be included as well.

Table 1: Connection Table at AP

CID	WM
C1	WM1
C2	WM1
C1	WM2

Table 2: Connection Table at WH

CID	WM	AP	XID
C1	WM1	AP1	5
C2	WM1	AP1	5
C1	WM2	AP1	6
C1	WM3	AP2	7

Table 3: Connection Table at IWF

CID	WM	WH	XID	IP/Port
C1	WM1	WH1	5	IP1/P1
C2	WM1	WH1	5	IP1/P2
C1	WM2	WH1	6	IP2/P3
C1	WM3	WH1	7	IP3/P1
C5	WM5	WH2	8	IP4/P1

The protocol stacks for dial-up users at home in a network as well as roaming users are illustrated in FIGS. 25-28. FIG. 25 depicts protocol stacks used for direct internet access by a fixed (i.e., non-moving) end system at home where a PPP protocol message terminates in the home IWF (typically collocated with the wireless hub) which relays message to and from an IP router and from there to the public internet. FIG. 26 depicts protocol stacks used for remote intranet access (i.e., either private corporate nets or an ISP) by a fixed (i.e., non-moving) end system at home where a PPP protocol message is relayed through the home IWF (typically collocated with the wireless hub) to a PPP server of the private corporate intranet or ISP. FIG. 27 depicts protocol stacks used for direct internet access by a roaming but fixed (i.e., non-moving) or a moving end system where the PPP protocol terminates in the home IWF (typically located in a mobile switching center of the home network) which relays message to and from an IP router. In FIG. 27, note how message traffic passes through a serving IWF (typically collocated with the wireless hub) in addition to the home IWF. FIG. 28 depicts protocol stacks used for remote intranet access (i.e., either private corporate nets or an ISP) by a roaming but fixed (i.e., non-moving) or a moving end system where a PPP protocol message is relayed through the home IWF (typically located in a mobile switching center of the home network) to a PPP server of the private corporate intranet or ISP. In FIG. 28, note how message traffic passes through a serving IWF (typically collocated with the wireless hub) in addition to the home IWF. When the serving IWF and the wireless hub are co-located in the same nest of computers or are even programmed into the same computer, it is not necessary to establish a tunnel using the XTunnel protocol between the serving IWF and the wireless hub.

Equivalent variations to these protocol stacks (e.g. the RLP can be terminated at the wireless hub rather than at the serving IWF or home IWF for mobiles at home) are also envisioned. If the IWF is located far from the wireless hub, and the packets can potentially be carried over a lossy IP network between the IWF and wireless hub, then it would be preferred to terminate the RLP protocol at the wireless hub Another variation is the Xtunnel between wireless hub and IWF need not be built on top of the UDP/IP. Xtunnels can be built using the Frame Relay/ATM link layer. However, the use of UDP/IP makes it easier to move the wireless hub and IWF software from one network to another

Furthermore, the PPP protocol can be terminated in a wireless modem and sent to one or more endsystems via an ethernet connection. As illustrated in FIG. 29, the wireless modem 300 receives the PPP protocol information and encapsulates the PPP payload in an ethernet frame to be transported to at least one of the end systems 304 and 306 via the internet connection 302.

DIX ethernet can be used for encapsulating the XWD MAC primitives but the system is not limited thereto. The ethernet frame format for XWD control frames is illustrated in Figure 30. The ethernet header contains a destination address, a source address and an ethernet type field. The destination address field contains the ethernet address of the MAC entity to which the primative is being sent. For MAC primitives invoked by the MAC user, this field will contain the ethernet address of the MAC user. For broadcast primitives, this address will be the ethernet broadcast address. The source address field contains the ethernet address of the MAC entity invoking the primitive. The ethernet type field contains the ethernet type for XWD. Possible values are XWD_Control for control frames and XWD_Data for data frames. These values must be different from all the ethernet type values that have been stnadardized and must be registered with the controlling authority.

The ethernet frame then has an XWD header field. The XWD header can be 16 bits long and will only be present for XWD control frames. The fields are illustrated in FIG. 31. The ethernet frame also contains a protocol header, a PPP payload field and a XWD MAC field. The header values for primitives using ethernet encapsulation are illustrated in Table 4 below.

Primitive Name	Destination Address	Source Address	Ethernet Type	XWD MAC Primitive
M_Discover.Req	Broadcast or unicast MAC Providider	MAC User	XWD_Control	0

M_Discover.Cnf	MAC User	MAC Provider	XWD_Control	1
M_OpenSap.Req	MAC Provider	MAC User	XWD_Control	2
M_OpenSap.Cnf	MAC User	MAC Provider	XWD_Control	3
M_CloseSap.Req	MAC Provider	MAC User	XWD_Control	4
M_CloseSap.Cnf	MAC User	MAC Provider	XWD_Control	5
M_EchoSap.Req	MAC User	MAC Provider	XWD_Control	6
M_EchoSap.Cnf	MAC Provider	MAC User	XWD_Control	7
M_Connect.Req	MAC Provider (modem only)	MAC User (end system only)	XWD_Control	8
M_Connect.Ind	MAC User (wireless hub only)	MAC Provider (AP only)	XWD_Control	9
M_Connect.Rsp	MAC Provider (AP only)	MAC User (wireless hub only)	XWD_Control	10
M_Connect.Cnf	MAC User (end system only)	MAC Provider (modem only)	XWD_Control	11
M_Disconect.Req	MAC Provider	MAC User	XWD_Control	12

In another alternative, the PPP protocol can be terminated in a wireless router and then sent on to at least one end system connected to a local area network (LAN). As illustrated in FIG. 32, the wireless router 350 receives the PPP protocol information via the wireless modem 352. The router 354 receives the PPP information from the wireless modem 352 and sends the PPP information to at least one of the end systems 356, 358, 360 via a LAN link 362.

Four types of handoff scenarios may occur, and they are labeled: (i) local mobility, (ii) micro mobility, (iii) macro mobility, and (iv) global mobility. In all four scenarios (in one embodiment of the invention), a route optimization option is not considered so that the locations of the home registration server and the ISP's PPP server do not change. In another embodiment of the system with route optimization, the ISP=s PPP server may change. However, this aspect is discussed below. In addition, the locations of the foreign registration server and IWF do not change in the first three scenarios.

The proposed IETF Mobile IP standard requires that whenever an end system changes the IP subnet to which it is attached, it sends a registration request message to a home agent in its home subnet. This message carries a care-of address where the end system can be reached in the new subnet. When traffic is sent, for example, from an ISP to an end system, the home agent intercepts the traffic that is bound for the end system as it arrives in the home subnet, and then forwards the traffic to the care-of address. The care-of address identifies a particular foreign agent in the foreign subnet. An end system's foreign agent can reside in the end system itself, or in a separate node that in turn forwards traffic to the end system (i.e., proxy registration agent). Mobile IP handoffs involve exchange of control messages between an end system's agent, the end system's home agent and potentially its corresponding hosts (CHs) (with route optimization option).

The proposed IETF Mobile IP standard would find it difficult to meet the latency and scalability goals for all movements in a large internetwork. However, the present hierarchical mobility management meets such goals. For small movements (e.g. a change of Access Points), only MAC-layer re-registrations are needed. For larger movements, network-layer re-registrations are performed. The present hierarchical mobility

management is different from the flat-structure used in the IETF proposed Mobile-IP standard as well as the serving/anchor inter-working function model used in cellular systems like CDPD (based on a standard sponsored by the Cellular Digital Packet Data forum).

As depicted in FIG. 33, the local mobility handoff handles end system (designated MN for mobile node) movement between APs that belong to the same wireless hub. Thus, only MAC layer re-registration is required. The end system receives a wireless hub advertisement from a new AP and responds with a registration request addressed to the new AP.

The new AP (i.e., the one that receives the registration request from the end system) creates new entries in its connection table and relays the registration message to its wireless hub. In local mobility handoffs, the wireless hub does not change. The wireless hub recognizes the end system's registration request as a MAC level registration request, and it updates its connection table to reflect the connection to the new AP. Then, the old AP deletes the connection entry from its connection table. There are at least three ways whereby the old AP can delete the old entries, namely (i) upon time out, (ii) upon receiving a copy of the relayed MAC layer association message from the new AP to the wireless hub (if this relay message is a broadcast message), and (iii) upon being informed by the wireless hub of the need to delete the entry.

As depicted in FIG. 34, the micro mobility handoff handles end system (designated MN for mobile node) movement between wireless hubs that belong to the same registration server and where the end system can still be served by the existing serving IWF. When an advertisement is received from a new wireless hub (through a new AP), the end system sends a message to request registration to the registration server. The registration request is relayed from the new AP to the new wireless hub to the registration server.

When the registration server determines that the existing IWF can still be used, the registration server sends a build XTunnel Request message to request the existing IWF to build an XTunnel to the new wireless hub. Later, the registration server sends a tear down XTunnel request message to request the existing IWF to tear down the

existing XTunnel with the old wireless hub. The build and tear XTunnel Request messages can be combined into one message. A foreign registration server does not forward the registration message to the home registration server since there is no change of IWF, either the serving IWF or home IWF.

Upon receiving a positive build XTunnel reply and a positive tear XTunnel reply from IWF, the registration server sends a registration reply to end system. As the registration reply reaches the new wireless hub, the connection table at the new wireless hub is updated to reflect the connection to the new AP. The new AP updates its MAC filter address table and connection table after receiving a message from the new wireless hub, and the registration reply is forwarded to the end system.

The registration server sends a release message to the old wireless hub. When the old wireless hub receives the release message, it updates its connection table and the MAC filter address table and connection table of the old AP.

As depicted in FIG. 35, the macro mobility handoff case handles movement between wireless hubs that involves a change of the serving IWF in the foreign network, but it does not involve a change in the registration server. When an advertisement is received from a new wireless hub (through a new AP), the end system sends a message to request a network layer registration to the registration server. The registration request is relayed from the new AP to the new wireless hub to the registration server.

The registration server recognizes that it is a foreign registration server when the end system does not belong to the present registration server's network. This foreign registration server determines the identity of the home registration server by using a request, preferably a Radius Access request (RA request), to the foreign directory server (like a big yellow pages) and then assigns an appropriate IWF to be the serving IWF, and it forwards a registration request to the home registration server, preferably through a Radius Access request (RA request), informing the home registration server of the newly selected IWF.

The home registration server authenticates the registration request by using a request, preferably a Radius Access request (RA request), to the home directory server. Upon authenticating the request and determining that the existing home IWF can still

be used, the home registration server instructs the home IWF to build a new I-XTunnel to the newly assigned serving IWF and to tear down the existing I-XTunnel to the old serving IWF. Upon receiving a positive build I-XTunnel reply and a positive tear I-XTunnel reply from the home IWF, the home registration server sends a registration reply to the foreign registration server.

The foreign registration server then instructs the newly assigned IWF to build an XTunnel to the new wireless hub. Upon receiving a positive build XTunnel reply, the foreign registration server instructs the old IWF to tear down the XTunnel to the old wireless hub. Upon receiving a positive build XTunnel reply and a positive tear XTunnel reply, the foreign registration server sends a registration reply to end system.

As the registration reply reaches the new wireless hub, the connection table at the new wireless hub is updated to reflect the connection to the new AP. The new AP updates its MAC filter address table and connection table after receiving a message from the new wireless hub, and the registration reply is forwarded to the end system.

The registration server sends a release message to the old wireless hub. When the old wireless hub receives the release message, it updates its connection table and the MAC filter address table, and the old AP updates its MAC filter address table and connection table after receiving a message from the old wireless hub.

The global mobility handoff case handles movement between wireless hubs that involves a change of registration servers. FIG. 36 depicts a global mobility handoff where the home IWF does not change, and FIG. 37 depicts a global mobility handoff where the home IWF changes. When an advertisement is received from a new wireless hub (through a new AP) in a new foreign network, the end system sends a message to request a network layer registration to the new foreign registration server. The registration request is relayed from the new AP to the new wireless hub to the new foreign registration server.

The registration server recognizes that it is a new foreign registration server when the end system does not belong to the present registration server's network. This foreign registration server determines the identity of the home registration server by using a request, preferably a Radius Access request (RA request), to the foreign

directory server (like a big yellow pages) and then assigns an appropriate IWF to be the serving IWF, and it forwards the registration request to the home registration server, preferably through a Radius Access request (RA request), informing the home registration server of the newly selected IWF.

The home registration server authenticates the registration request by using a request, preferably a Radius Access request (RA request), to the home directory server. Upon authenticating the request and determining that the existing home IWF can still be used (FIG. 36), the home registration server instructs the home IWF to build a new I-XTunnel to the serving IWF newly assigned by the new foreign registration server. The home registration server also sends a de-registration message to the old foreign registration server and instructs the home IWF to tear down the existing I-XTunnel to the existing serving IWF of the old foreign network. Upon receiving a positive build I-XTunnel reply and a positive tear I-XTunnel reply from the home IWF, the home registration server sends a registration reply to the new foreign registration server.

The new foreign registration server then instructs the newly assigned IWF to build an XTunnel to the new wireless hub. Upon receiving a positive build XTunnel reply, the foreign registration server sends a registration reply to end system. As the registration reply reaches the new wireless hub, the connection table at the new wireless hub is updated to reflect the connection to the new AP. The new AP updates its MAC filter address table and connection table after receiving a message from the new wireless hub, and the registration reply is forwarded to the end system.

The old foreign registration server instructs the old IWF to tear down the XTunnel to the old wireless hub. Upon receiving a positive tear XTunnel reply or contemporaneously with the tear down XTunnel request, the old foreign registration server sends a release message to the old wireless hub. When the old wireless hub receives the release message, it updates its connection table and the MAC filter address table, and the old AP updates its MAC filter address table and connection table after receiving a message from the old wireless hub.

Alternatively, after the home registration server authenticates the registration request from the new foreign registration server and determines that the existing home

IWF cannot be used (FIG. 37), the home registration server chooses a new home IWF and instructs the new home IWF to build a new level 2 tunnel protocol tunnel (L2TP tunnel) to the present PPP server (e.g., the PPP server in a connected ISP intranet). Then, the home registration server instructs the old home IWF to transfer its L2TP tunnel traffic to the new home IWF.

Then the home registration server instructs the new home IWF to build a new I-XTunnel to the serving IWF newly assigned by the new foreign registration server. The home registration server also sends a de-registration message to the old foreign registration server and instructs the home IWF to tear down the existing I-XTunnel to the existing serving IWF of the old foreign network. Upon receiving a positive build I-XTunnel reply and a positive tear I-XTunnel reply from the home IWF, the home registration server sends a registration reply to the new foreign registration server.

The new foreign registration server then instructs the newly assigned IWF to build an XTunnel to the new wireless hub. Upon receiving a positive build XTunnel reply, the foreign registration server sends a registration reply to end system. As the registration reply reaches the new wireless hub, the connection table at the new wireless hub is updated to reflect the connection to the new AP. The new AP updates its MAC filter address table and connection table after receiving a message from the new wireless hub, and the registration reply is forwarded to the end system.

The old foreign registration server instructs the old IWF to tear down the XTunnel to the old wireless hub. Upon receiving a positive tear XTunnel reply or contemporaneously with the tear down XTunnel request, the old foreign registration server sends a release message to the old wireless hub. When the old wireless hub receives the release message, it updates its connection table and the MAC filter address table, and the old AP updates its MAC filter address table and connection table after receiving a message from the old wireless hub.

End systems constructed according to the present system interoperate with networks constructed according to the proposed IETF Mobile-IP standards, and end systems constructed according to the proposed IETF Mobile-IP standards interoperate with networks constructed according to the present invention.

Differences between the present system and the IETF Mobile-IP (RFC2002, a standards document) include:

(i) The present systemists a hierarchical concept for mobility management rather than a flat structure as in the proposed IETF Mobile-IP standard. Small mobility within a small area does not result in a network level registration. Micro mobility involves setting up of a new Xtunnel and tearing down of an existing Xtunnel. Global mobility, at the minimum, involves setting up of a new I-XTunnel and tearing down of an existing I-Xtunnel apart from the setting up/tearing down of XTunnel. Global mobility sometimes also involves setting up a new L2TP Tunnel and transferring of L2TP state from the existing L2TP Tunnel to the new L2TP Tunnel.

(ii) In the present invention, a user name plus a realm is used to identify a remote dial-up user rather than a fixed home address as in the case of the proposed IETF Mobile-IP standard.

(iii) In the present invention, registration and routing functions are carried out by separate entities. The two functions are carried out by the home agent in the proposed IETF Mobile IP standard, and both functions are carried out by the foreign agent in the proposed IEFT Mobile IP standard. In contrast, in an embodiment of the present invention, registration is carried out in the registration server and routing functions are carried out by both the home and foreign IWF and the wireless hub (also referred to as the access hub).

(iv) The present system utilizes three tunnels per PPP session. The XTunnel is more of a link-layer tunnel between the wireless hub and the serving IWF. The I-XTunnel between the serving IWF and the home IWF is more like the tunnel between home and foreign agents in the proposed IETF Mobile-IP standard. But it also has additional capabilities beyond the tunnels proposed by the Mobile-IP standard. The L2TP tunnel is used only when home IWF is not a PPP server. The number of these

tunnels may be reduced by combining some functions in the same nodes as described earlier.

(v) In the present invention, wireless registration occurs before PPP session starts while in the proposed IETF Mobile-IP standard, Mobile-IP registration occurs after PPP session enters into the open state.

(vi) In the present invention, the network entity that advertises the agent advertisement (i.e., the wireless hub) is not on a direct link to the end systems whereas for the proposed IETF Mobile-IP standard, the agent advertisement must have a TTL of 1 which means that the end systems have a direct link with the foreign agent. In addition, the agent advertisement in the present systems not an extension to the ICMP router advertisements as in the proposed IETF Mobile-IP standard.

End systems in the present invention, should support agent solicitation. When an end system in the present system visits a network which is supporting the proposed IETF Mobile-IP standard, it waits until it hears an agent advertisement. If it does not receive an agent advertisement within a reasonable time frame, it broadcasts an agent solicitation.

In the present invention, network operators may negotiate with other networks that support the proposed IETF Mobile-IP standard such that home addresses can be assigned to the end systems of the present system that wish to use other networks. When the end system of the present system receives the agent advertisement, it can determine that the network it is visiting is not an a network according to the present system and hence uses the assigned home address to register.

For networks supporting the proposed IETF Mobile-IP standard, the PPP session starts before Mobile-IP registration, and the PPP server is assumed to be collocated with the foreign agent in such networks. In one embodiment, an SNAP header is used to encapsulate PPP frames in the MAC frames of the present system(in a manner similar to Ethernet format), and the foreign agent interprets this format as a proprietary PPP format over Ethernet encapsulation. Thus, the end system of the present system and its PPP peer can enter into an open state before the foreign agent

starts transmitting an agent advertisement, and the end system of the present system can register.

To allow end systems supporting the proposed IETF Mobile-IP standard to work in networks of the type of the present invention, such mobiles are at least capable of performing similar MAC layer registrations. By making the agent advertisement message format similar to the proposed Mobile-IP standard agent advertisement message format, a visiting end system can interpret the agent advertisement and register with a wireless hub. In the present invention, registration request and reply messages are similar to the proposed IETF Mobile-IP standard registration request and reply messages (without any unnecessary extensions) so that the rest of the mobility management features of the present system are transparent to the visiting end systems.

Since end systems supporting the proposed IETF Mobile-IP standard expect a PPP session to start before Mobile-IP registration, an optional feature in wireless hubs of the present system starts to interpret PPP LCP, NCP packets after MAC-layer registrations.

To avoid losing traffic during handoffs, the mobility management of the present systemists the make before break concept. For local mobility, a make before break connection is achieved by turning the MAC-layer registration message relayed by the new AP to the wireless hub into a broadcast message. That way, the old AP can hear about the new registration and forward packets destined for the end system that have not been transmitted to the new AP.

For micro mobility, information about the new wireless hub is included in the Tear XTunnel message exchanged between the serving IWF and the old WH. That way, the old wireless hub can forward buffered packets to the new wireless hub upon hearing a TearXTunnel message from the serving IWF. Alternatively, the RLP layer at the IWF knows the sequence number that has been acknowledged by the old wireless hub so far.

At the same time, the IWF knows the current send sequence number of the latest packet sent to the old wireless hub. Therefore, the IWF can forward those packets that are ordered in between these two numbers to the new wireless hub before sending newer packets to the new wireless hub. The RLP layer is assumed to be able to filter duplicate

packet. The second approach is probably preferable to the first approach for the old wireless hub may not be able to communicate with one another directly.

For macro mobility, the old serving IWF can forward packets to the new serving IWF, in addition to the packet forwarding done from the old wireless hub to the new wireless. All we need to do is to forward the new serving IWF identity to the new serving IWF in the tear down I-XTunnel message. Another way to achieve the same result is to let the home IWF forward the missing packets to the new serving IWF rather than asking the old serving IWF to do the job since the home IWF knows the I-XTunnel sequence number last acknowledged by the old serving IWF and the current I-XTunnel sequence number sent by the home IWF.

The method of estimating how much buffer should be allocated per mobile per AP per wireless hub per IWF such that the traffic loss between handoffs can be minimized is to let the end system for the AP for the wireless hub for the IWF estimate the packet arrival rate and the handoff time. This information is passed to the old AP of the wireless hub of the IWF to determine how much traffic should be transferred to the new AP of the wireless hub of the IWF, respectively, upon handoffs.

To achieve route optimization in the present invention, the end system chooses the PPP server closest to the serving IWF. Without route optimization, excessive transport delays and physical line usage may be experienced.

For example, an end system subscribed to a home network in New York City may roam to Hong Kong. To establish a link to a Hong Kong ISP, the end system would have a serving IWF established in a wireless hub in Hong Kong and a home IWF established in the home network in New York City. A message would then be routed from the end system (roamed to Hong Kong) through the serving IWF (in Hong Kong) and through the home IWF (in New York City) and back to the Hong Kong ISP.

A preferred approach is to connect from the serving IWF (in Hong Kong) directly to the Hong Kong ISP. The serving IWF acts like the home IWF. In this embodiment, roaming agreements exist between the home and foreign wireless providers. In addition, the various accounting/billing systems communicate with one another automatically such that billing information is shared. Accounting and billing

information exchange may be implemented using standards such as the standard proposed by the ROAMOPS working group of the IETF.

However, the serving IWF must still discover the closest PPP server (e.g., the Hong Kong ISP). In the present embodiment, the foreign registration server learns of the end system's desire to connect to a PPP server (e.g., a Hong Kong ISP) when it receives a registration request from the end system. When the foreign registration server determines that the serving IWF is closer to the desired PPP server (e.g., the Hong Kong ISP) than the home IWF is, the foreign registration server instructs the serving IWF to establish an L2TP tunnel to its nearest PPP server (in contrast to the PPP server closest to the home registration server and home IWF). Then, the foreign registration server informs the home registration server that the end system is being served by the serving IWF and the foreign PPP.

In an alternative embodiment, the foreign registration server determines that the serving IWF is closer to the desired PPP server (e.g., the Hong Kong ISP) than the home IWF is, when it receives a registration request from the end system. The foreign registration server relays the registration request message to the home registration server with an attached message indicating the serving IWF information and a notification that route optimization is preferred. At the same time, the foreign registration server instructs the serving IWF to establish an L2TP tunnel to the PPP server. Upon approving the registration request, the home registration server instructs the home IWF to transfer the L2TP state to the foreign IWF.

Having described preferred embodiments of a novel network architecture with wireless end users able to roam (which are intended to be illustrative and not limiting), it is noted that modifications and variations can be made by persons skilled in the art in light of the above teachings. For example, connection links described herein may make reference to known connection protocols (e.g., IP, TCP/IP, L2TP, IEEE 802.3, etc.); however, the system contemplates other connection protocols in the connections links that provide the same or similar data delivery capabilities. Acting agents in the above described embodiments may be in the form of software controlled processors or may be other form of controls (e.g., programmable logic arrays, etc.). Acting agents may be grouped as described above or grouped otherwise

in keeping with the connection teachings described herein and subject to security and authentication teachings as described herein. Furthermore, a single access point, access hub (i.e., wireless hub) or inter-working function unit (IWF unit) may provide multi-channel capability. Thus, a single access point or access hub or IWF unit may act on traffic from multiple end systems, and what is described herein as separate access points, access hubs or IWF units contemplates equivalence with a single multi-channel access point, access hub or IWF unit. It is therefore to be understood that changes may be made in the particular embodiments of the system disclosed which are within the scope and spirit of the systems defined by the appended claims.

Having thus described the system with the details and particularity required by the patent laws, what is claimed and desired protected by Letters Patent is set forth in the appended claims.

4. Brief Description Of Drawings

The system will be described in detail in the following description of preferred embodiments with reference to the following figures wherein:

FIG. 1 is a configuration diagram of a known remote access architecture through a public switched telephone network;

FIG. 2 is a configuration diagram of a remote access architecture through a wireless packet switched data network according to the present invention;

FIG. 3 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing a roaming scenario;

FIG. 4 is a configuration diagram of a base station with local access points;

FIG. 5 is a configuration diagram of a base station with remote access points;

FIG. 6 is a configuration diagram of a base station with remote access points, some of which are connected using a wireless trunk connection;

FIG. 7 is a diagram of a protocol stack for a local access point;

FIG. 8 is a diagram of a protocol stack for a remote access point with a wireless trunk;

FIG. 9 is a diagram of a protocol stack for a relay function in the base station for supporting remote access points with wireless trunks;

FIG. 10 is a diagram of protocol stacks for implementing the relay function depicted in FIG. 9;

FIG. 11 is a diagram of protocol stacks for a relay function in the base station for supporting local access points;

FIG. 12 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing a first end system registering in the home network from the home network and a second system registering in the home network from a foreign network using a home inter-working function for an anchor;

FIG. 13 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing a first end system registering in the home network from the home network and a second system registering in the home network from a foreign network using a serving inter-working function for an anchor;

FIG. 14 is a ladder diagram of the request and response messages to register in a home network from a foreign network and to establish, authenticate and configure a data link;

FIG. 15 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing registration requests and responses for registering a mobile in a home network from the home network;

FIG. 16 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing registration requests and responses for registering a mobile in a home network from a foreign network;

FIG. 17 is a configuration diagram of protocol stacks showing communications between an end system in a home network and an inter-working function in the home network where the cell site has local access points;

FIG. 18 is a configuration diagram of protocol stacks showing communications between an end system in a home network and an inter-working function in the home network where the cell site has remote access points coupled to a wireless hub through a wireless trunk;

FIG. 19 is a configuration diagram of protocol stacks showing communications between a base station coupled to a roaming end system and a home inter-working function;

FIG. 20 is a configuration diagram of protocol stacks showing communications between an end system in a home network through an inter-working function in the home network to an internet service provider;

FIG. 21 is a configuration diagram of protocol stacks showing communications between an end system in a foreign network and a home registration server in a home network during the registration phase;

FIG. 22 is a processing flow diagram showing the processing of accounting data through to the customer billing system;

FIGS. 23 and 24 are ladder diagrams depicting the registration process for an end system in a home network and in a foreign network, respectively;

FIGS. 25 and 26 are protocol stack diagrams depicting an end system connection in a home network where a PPP protocol terminates in an inter-working function of the home network and where the PPP protocol terminates in an ISP or intranet, respectively;

FIGS. 27 and 28 are protocol stack diagrams depicting an end system connection in a foreign network where a PPP protocol terminates in an inter-working function of the foreign network and where the PPP protocol terminates in an ISP or intranet, respectively;

FIG. 29 illustrates end systems connected via ethernet to a wireless modem where PPP protocol is encapsulated in an ethernet frame;

FIG. 30 illustrates an ethernet frame format;

FIG. 31 illustrates XWD Header fields;

FIG. 32 illustrates end systems connected via a local area network to a wireless router where PPP protocol terminates at the wireless router;

FIGS. 33, 34 and 35 are ladder diagrams depicting a local handoff scenario, a micro handoff scenario and a macro handoff scenario, respectively;

FIG. 36 is a ladder diagram depicting a global handoff scenario where the foreign registration server changes and where home inter-working function does not change; and

FIG. 37 is a ladder diagram depicting a global handoff scenario where both the foreign registration server and the home inter-working function change.

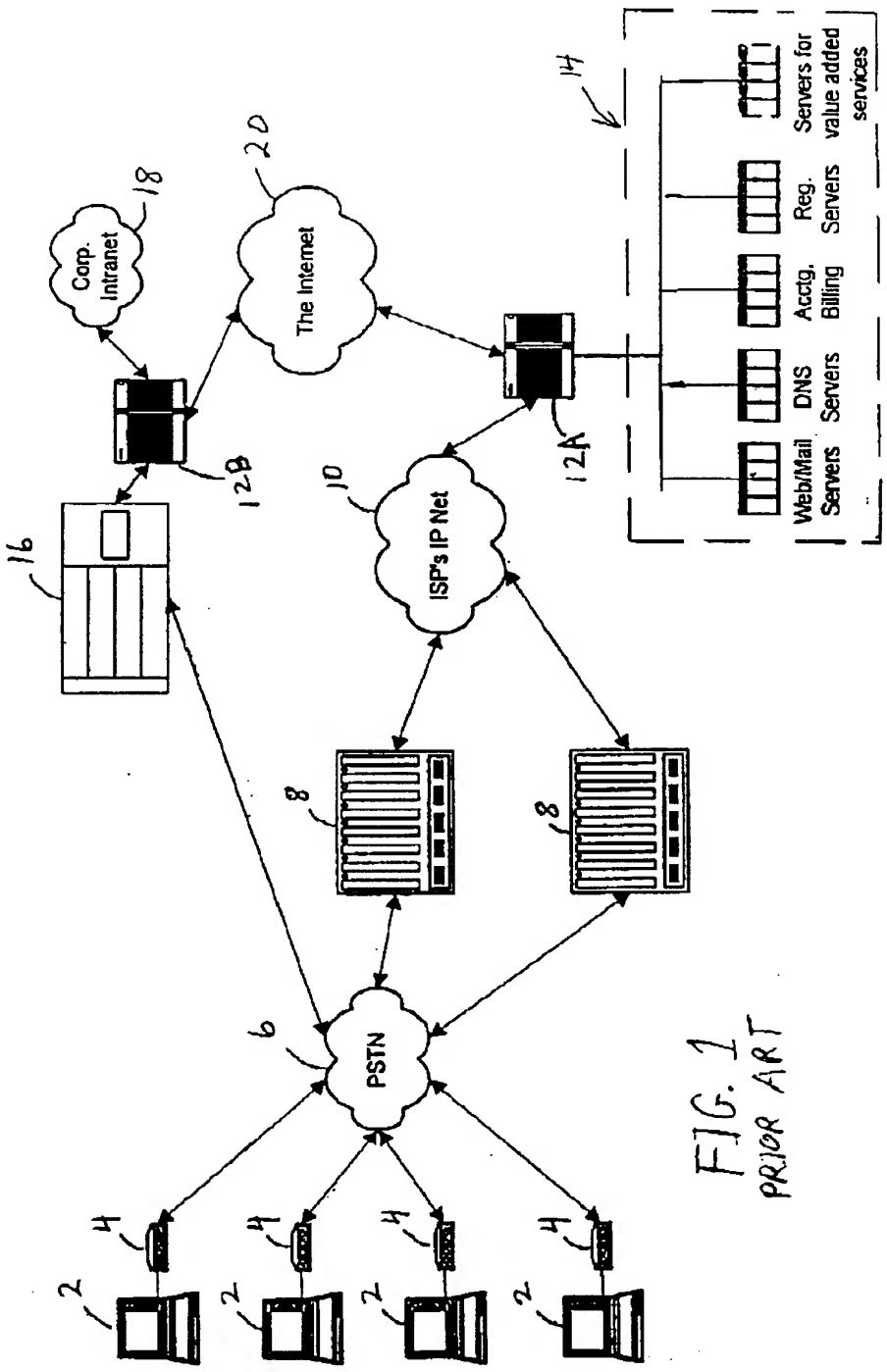


FIG. 1
PRIOR ART

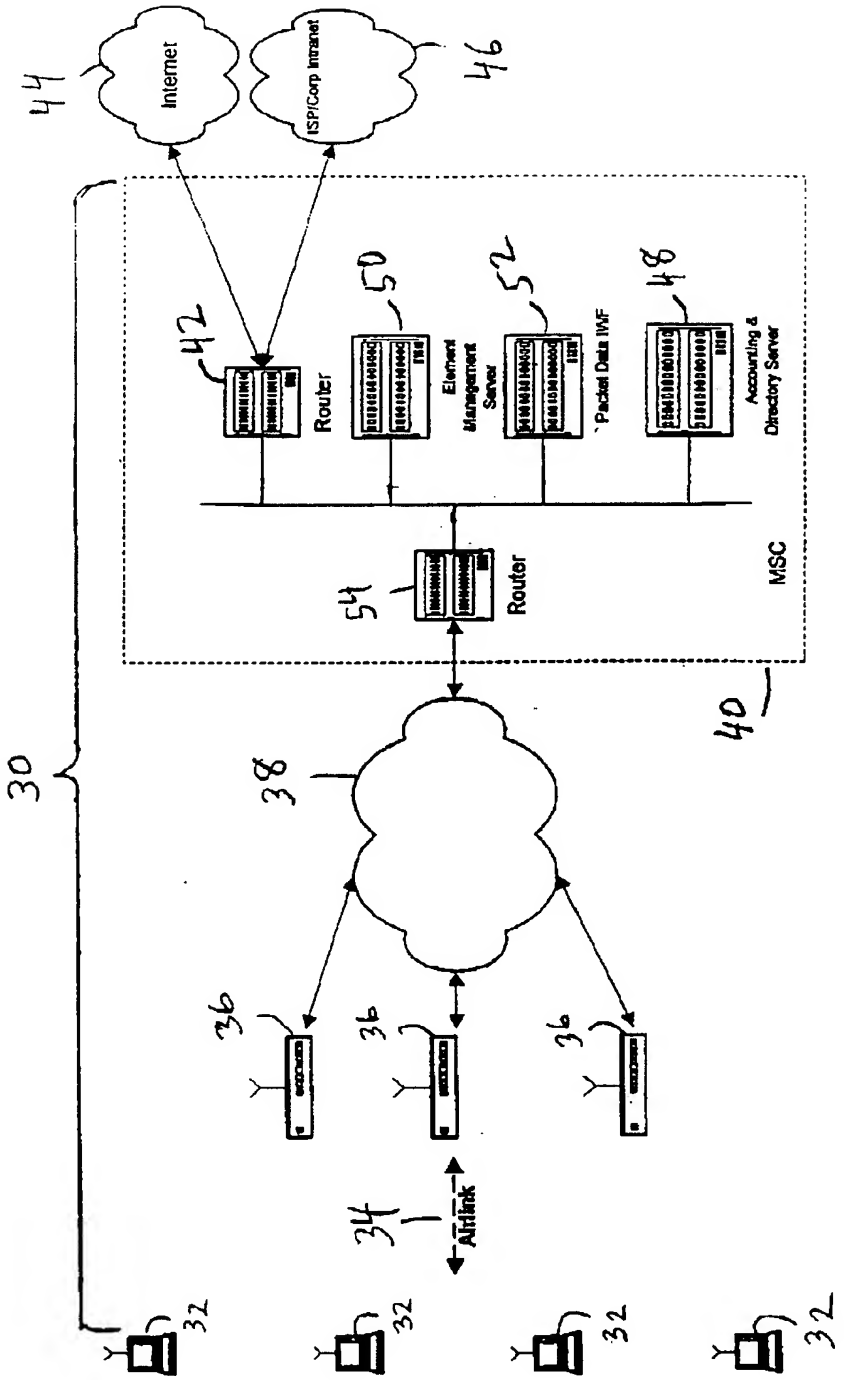

Internet
ISP/Corp Intranet
44
46
42
50
52
48
Router
Element Management Server
Packet Data IWF
Accounting & Directory Server
54
Router
MSC
40
30
38
36
36
36
34
Airlink
32
32
32
32

FIG. 2

FIG. 3

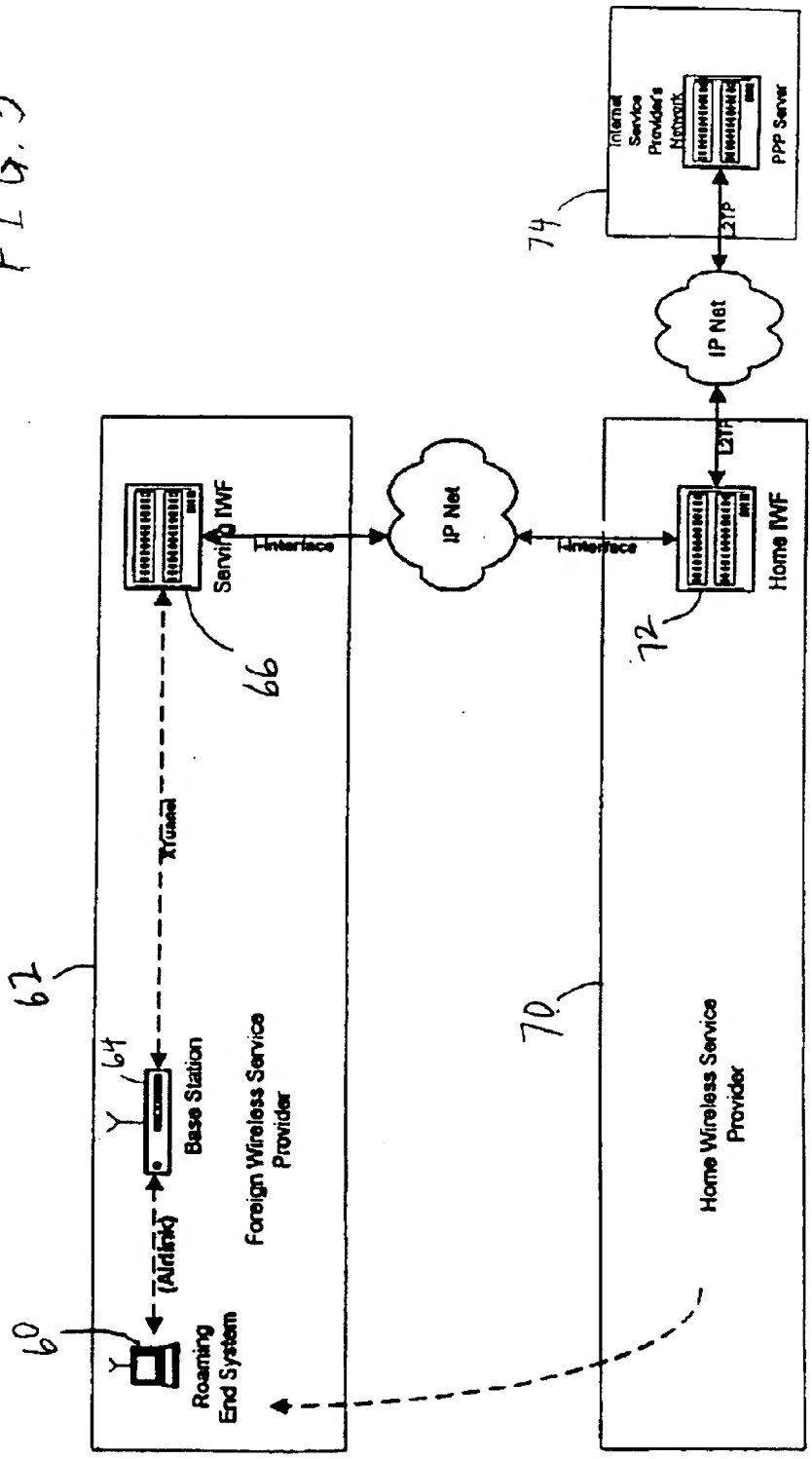

Internet Service Provider's Network
PPP Server
74
L2TP
IP Net
L2TP
Home IWF
72
Interface
IP Net
Interface
Serving IWF
66
Trusted
62
Base Station
64
Foreign Wireless Service Provider
70
Home Wireless Service Provider
(Air link)
60
Roaming End System

FIG. 4

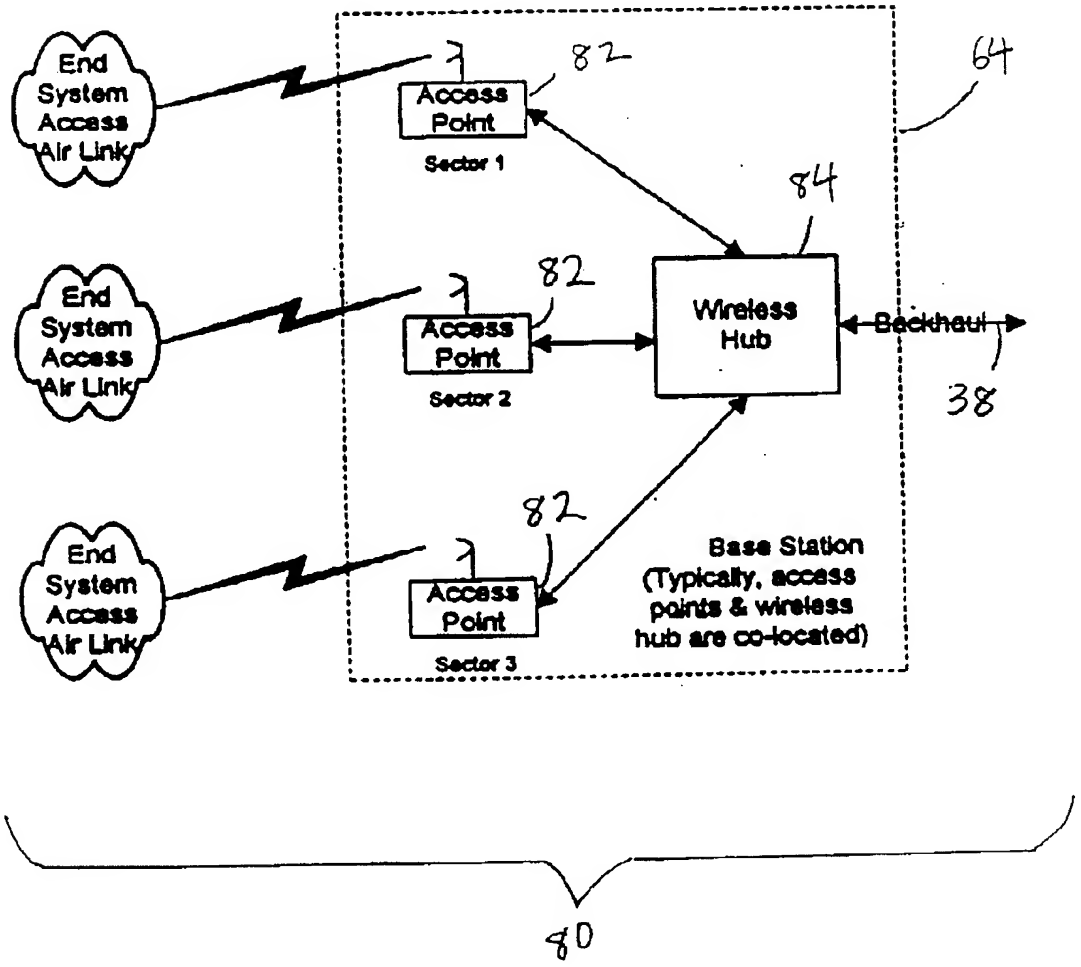

End System Access Air Link
End System Access Air Link
End System Access Air Link
Access Point
Sector 1
Access Point
Sector 2
Access Point
Sector 3
82
82
82
64
84
Wireless Hub
Backhaul
38
Base Station (Typically, access points & wireless hub are co-located)
80

FIG 5

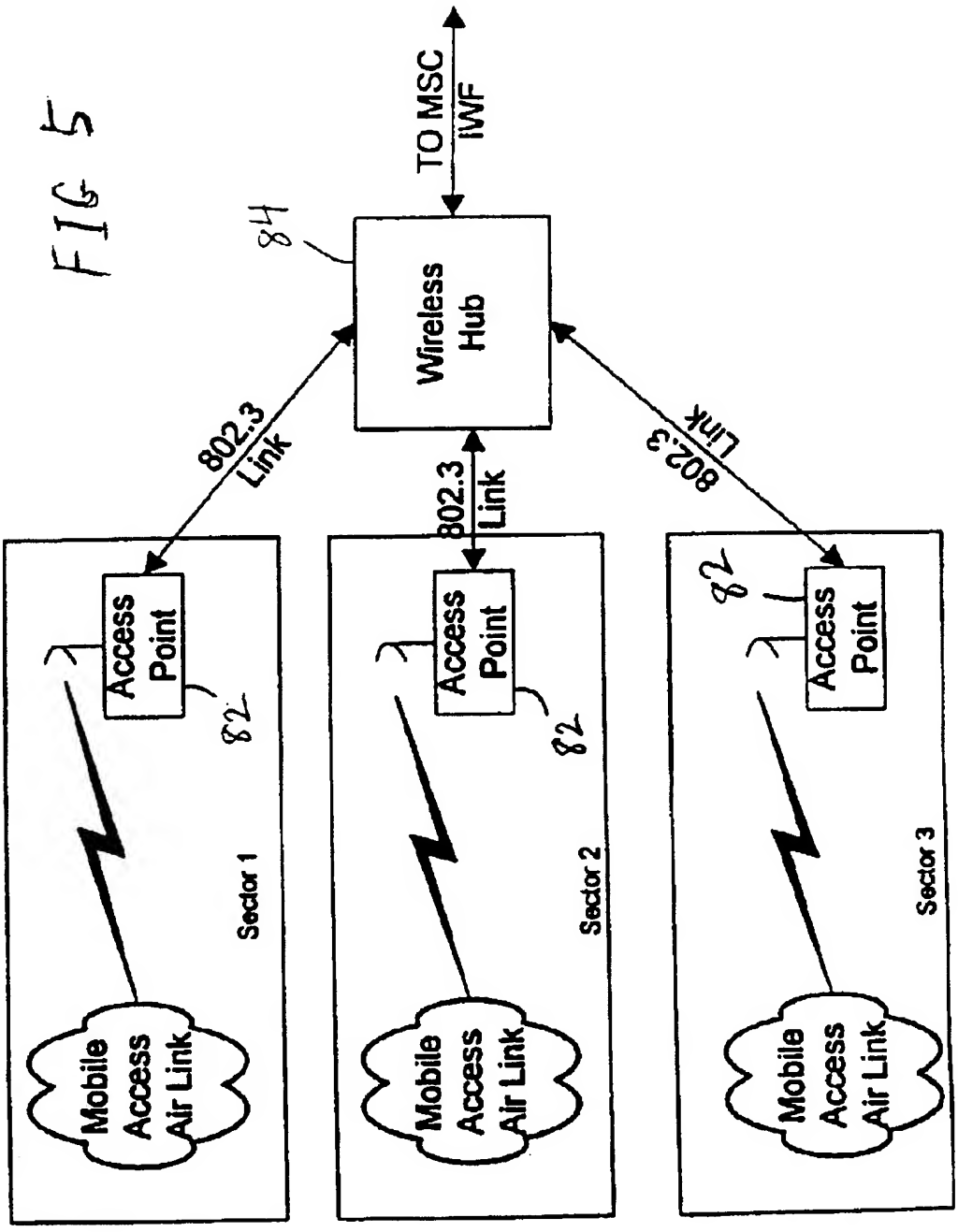
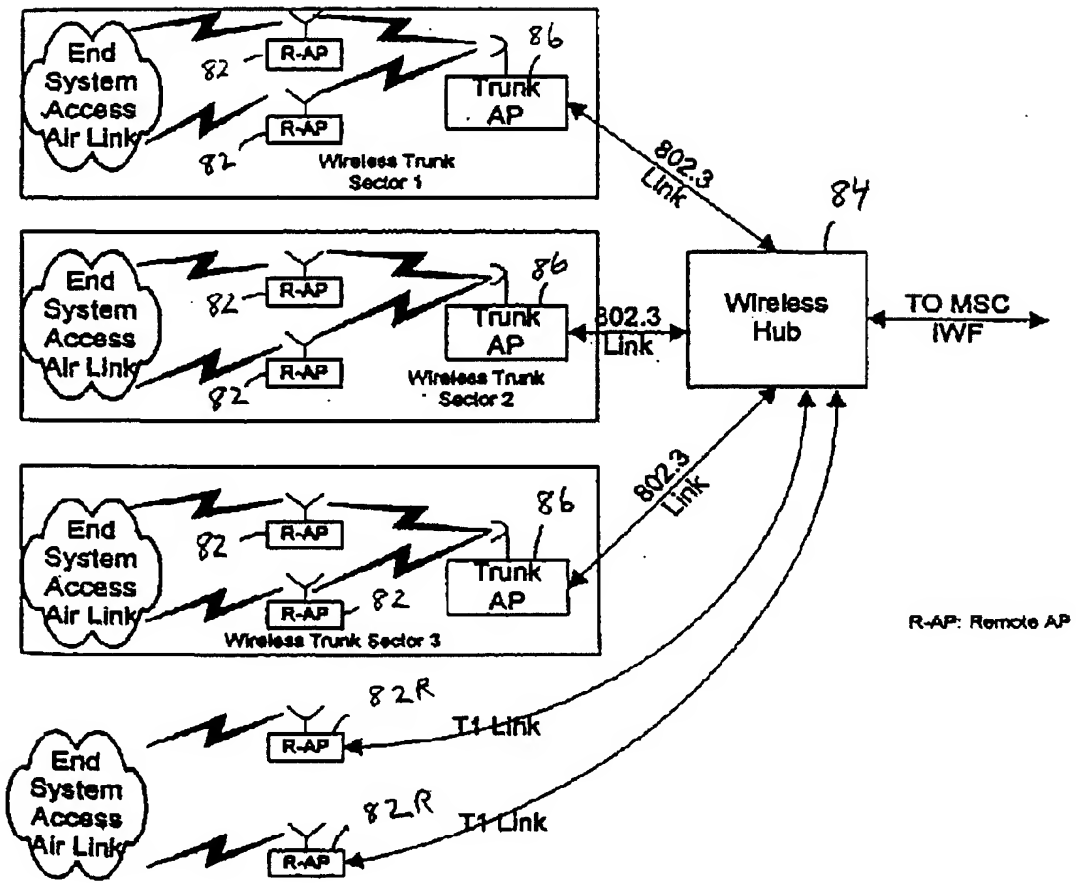

TO MSC
IWF
84
Wireless Hub
802.3 Link
802.3 Link
802.3 Link
Access Point
82
Mobile Access Air Link
Sector 1
Sector 2
Sector 3

FIG. 6


End System Access Air Link
R-AP
82
86
Trunk AP
Wireless Trunk Sector 1
802.3 Link
84
Wireless Hub
TO MSC IWF
Wireless Trunk Sector 2
Wireless Trunk Sector 3
R-AP: Remote AP
82R
T1 Link

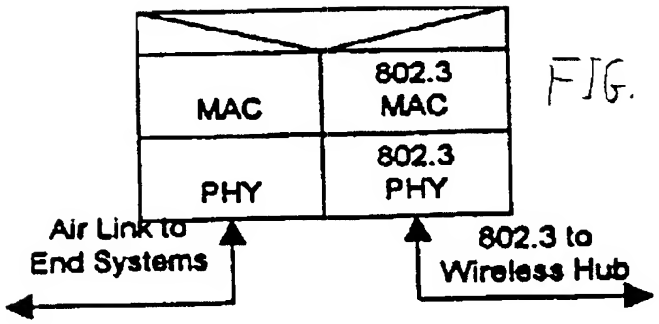


FIG. 7

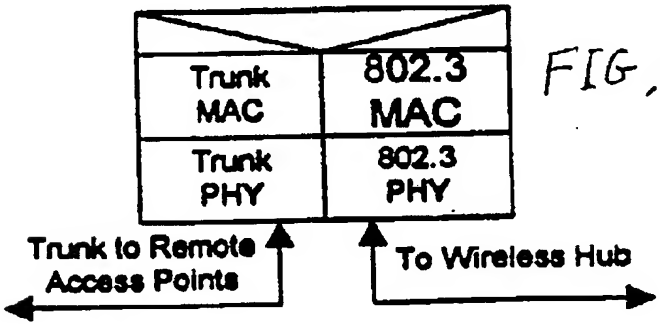


FIG. 8

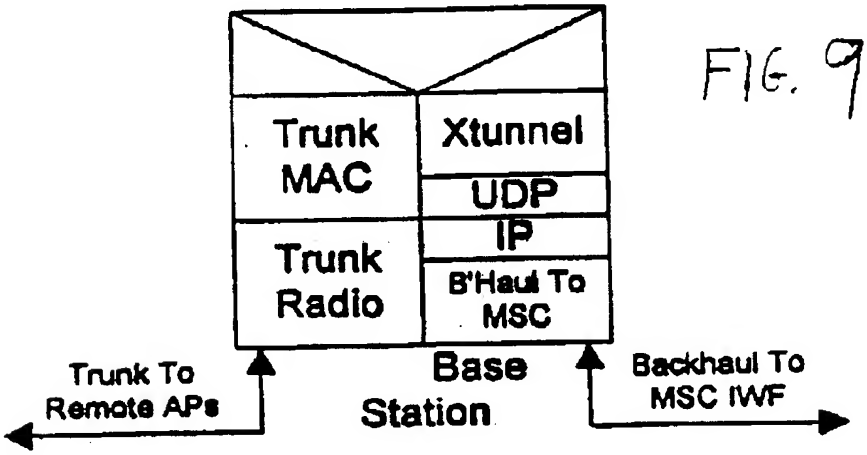


FIG. 9

FIG. 10

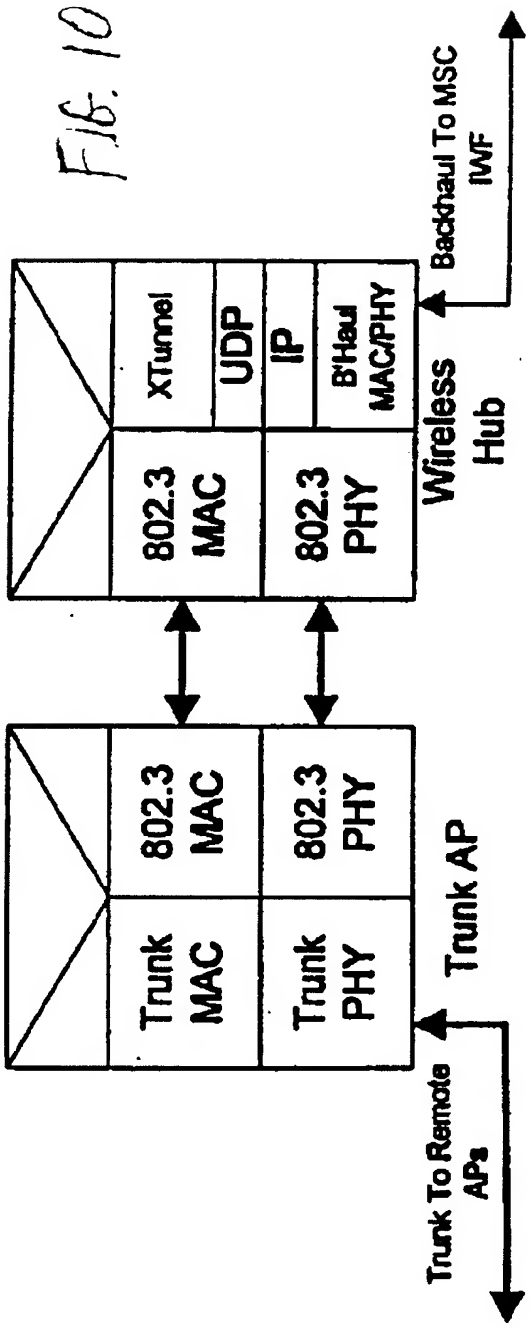
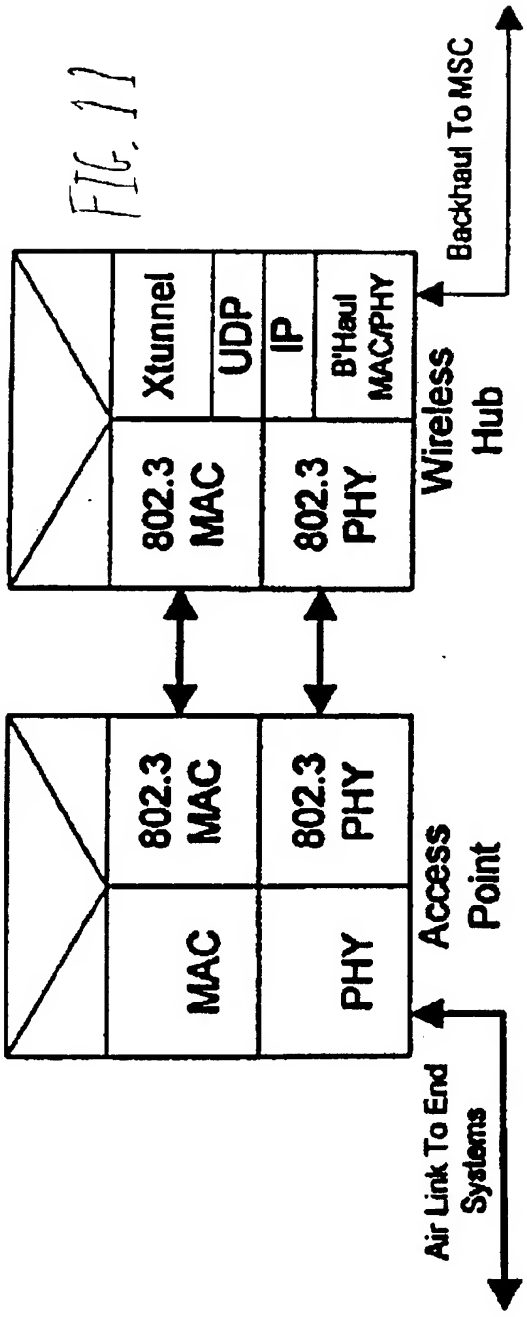

Backhaul To MSC IWF
Wireless Hub
XTunnel
UDP
IP
B'Haul MAC/PHY
802.3 MAC
802.3 PHY
Trunk AP
Trunk MAC
Trunk PHY
Trunk To Remote APs

FIG. 11


Backhaul To MSC
Xtunnel
UDP
IP
B'Haul MAC/PHY
802.3 MAC
802.3 PHY
Wireless Hub
802.3 MAC
802.3 PHY
MAC
PHY
Access Point
Air Link To End Systems

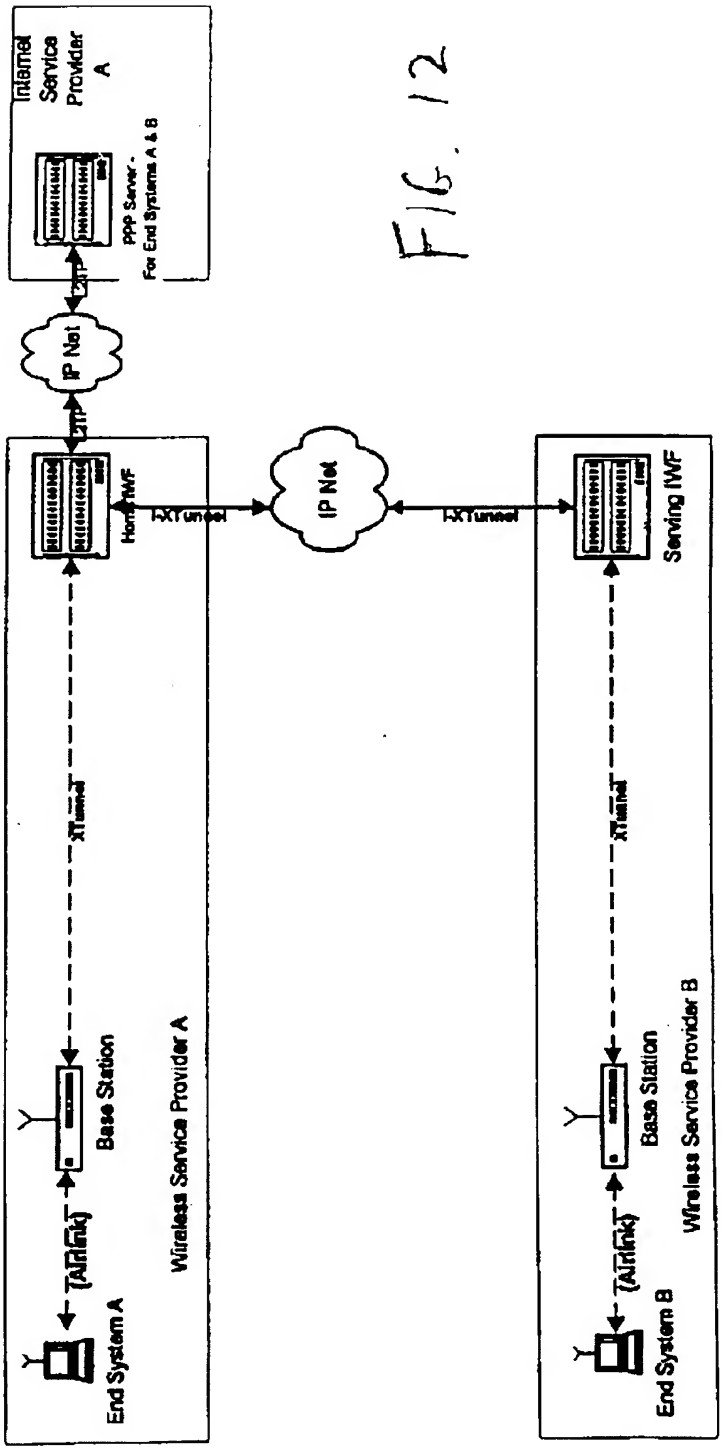

Internet Service Provider A
PPP Server - For End Systems A & B
IP Net
Home IWF
I-XTunnel
IP Net
I-XTunnel
Serving IWF
XTunnel
XTunnel
Base Station
Base Station
Wireless Service Provider A
Wireless Service Provider B
AirLink
AirLink
End System A
End System B

FIG. 12

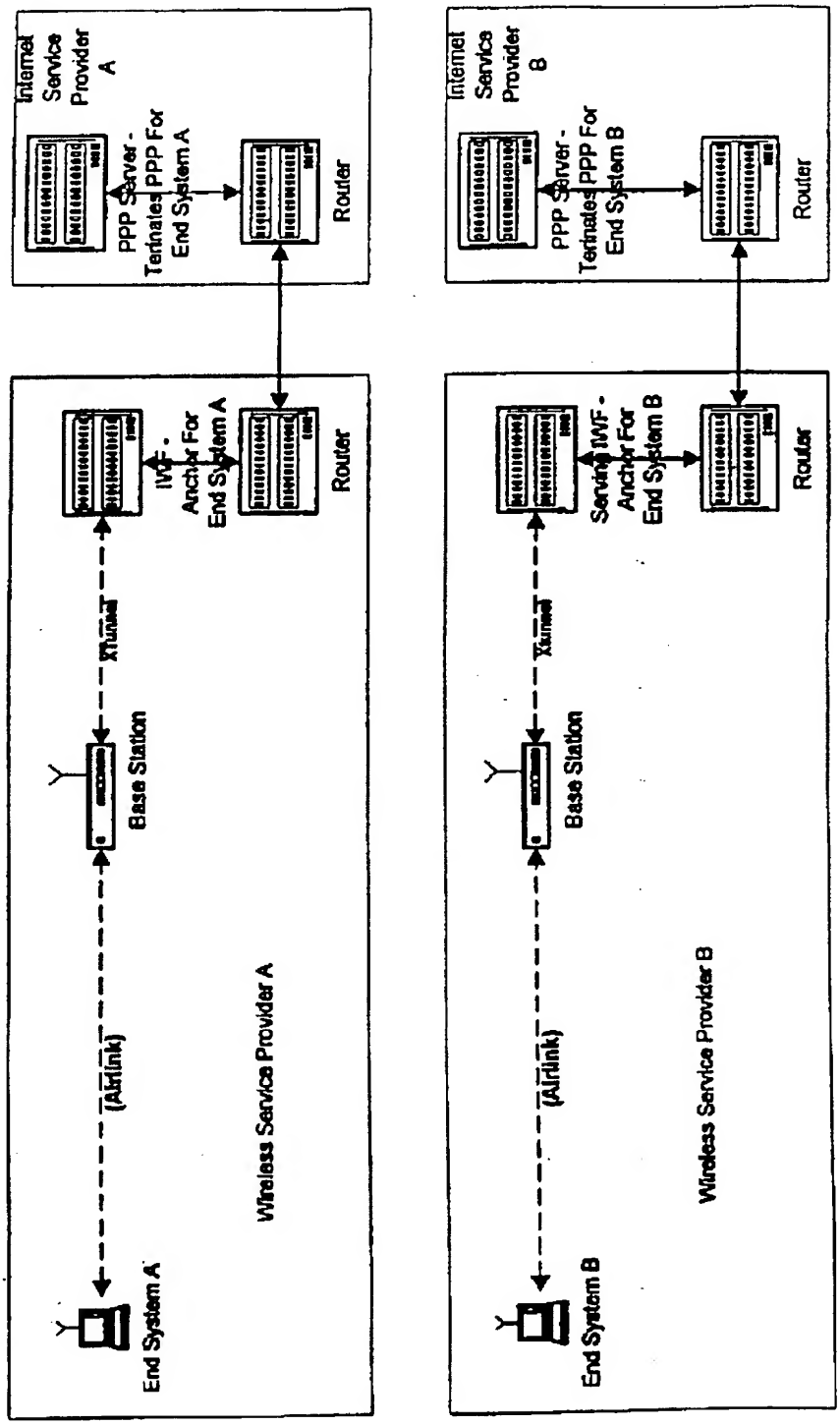

Internet Service Provider A
PPP Server - Terinates PPP For End System A
Router
IWF - Anchor For End System A
Router
Xunnel
Base Station
(Airlink)
End System A
Wireless Service Provider A
Internet Service Provider B
PPP Server - Terinates PPP For End System B
Router
Serving IWF - Anchor For End System B
Router
Xunnel
Base Station
(Airlink)
End System B
Wireless Service Provider B

FIG 13

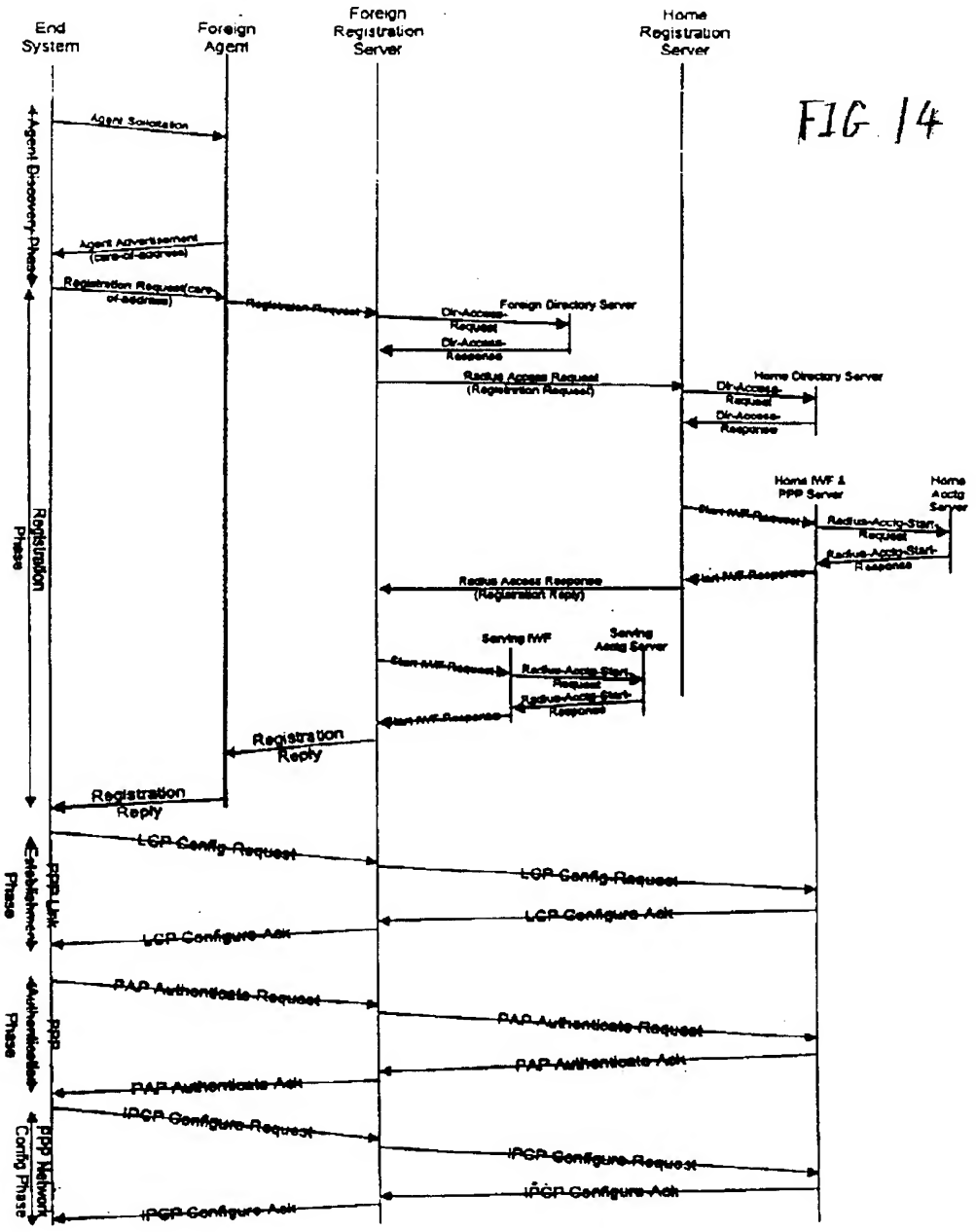

End System
Foreign Agent
Foreign Registration Server
Home Registration Server
Agent Solicitation
Agent Discovery Phase
Agent Advertisement (care-of-address)
Registration Request(care-of-address)
Registration Request
Foreign Directory Server
Dir-Access-Request
Dir-Access-Response
Radius Access Request (Registration Request)
Home Directory Server
Dir-Access-Request
Dir-Access-Response
Home IWF & PPP Server
Home Acctg Server
Start-IWF-Request
Radius-Acctg-Start-Request
Radius-Acctg-Start-Response
Start-IWF-Response
Radius Access Response (Registration Reply)
Registration Phase
Serving IWF
Serving Acctg Server
Start-IWF-Request
Radius-Acctg-Start-Request
Radius-Acctg-Start-Response
Start-IWF-Response
Registration Reply
Registration Reply
LCP Config Request
LCP Config Request
LCP Configure-Ack
LCP Configure-Ack
PPP Link Establishment Phase
PAP Authenticate-Request
PAP Authenticate-Request
PAP Authenticate-Ack
PAP Authenticate-Ack
PPP Authentication Phase
IPCP Configure-Request
IPCP Configure-Request
IPCP Configure-Ack
IPCP Configure-Ack
PPP Network Config Phase

FIG 14

FIG. 15

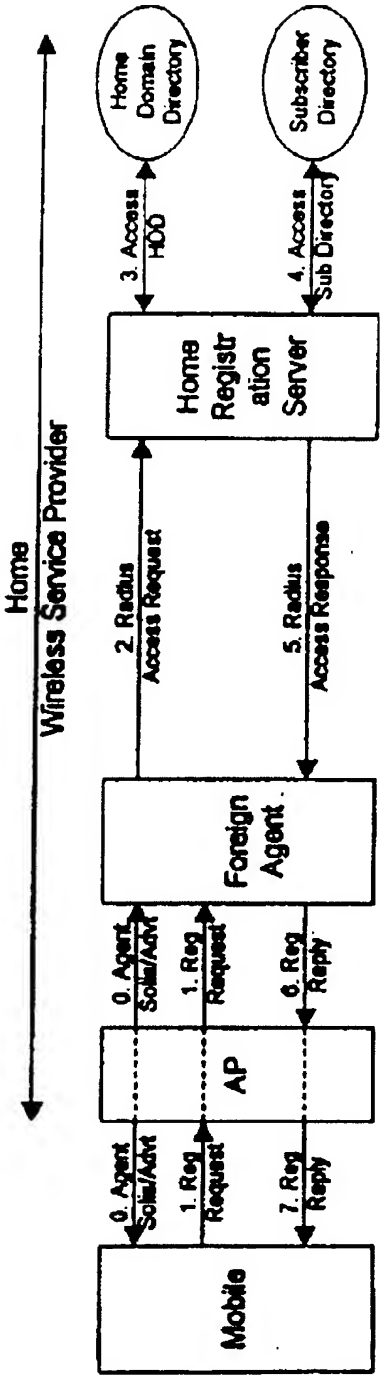

Home Wireless Service Provider
Home Domain Directory
Subscriber Directory
3. Access HDD
4. Access Sub Directory
Home Registration Server
2. Radius Access Request
5. Radius Access Response
Foreign Agent
0. Agent Solic/Advt
1. Reg Request
6. Reg Reply
AP
0. Agent Solic/Advt
1. Reg Request
7. Reg Reply
Mobile

FIG. 16

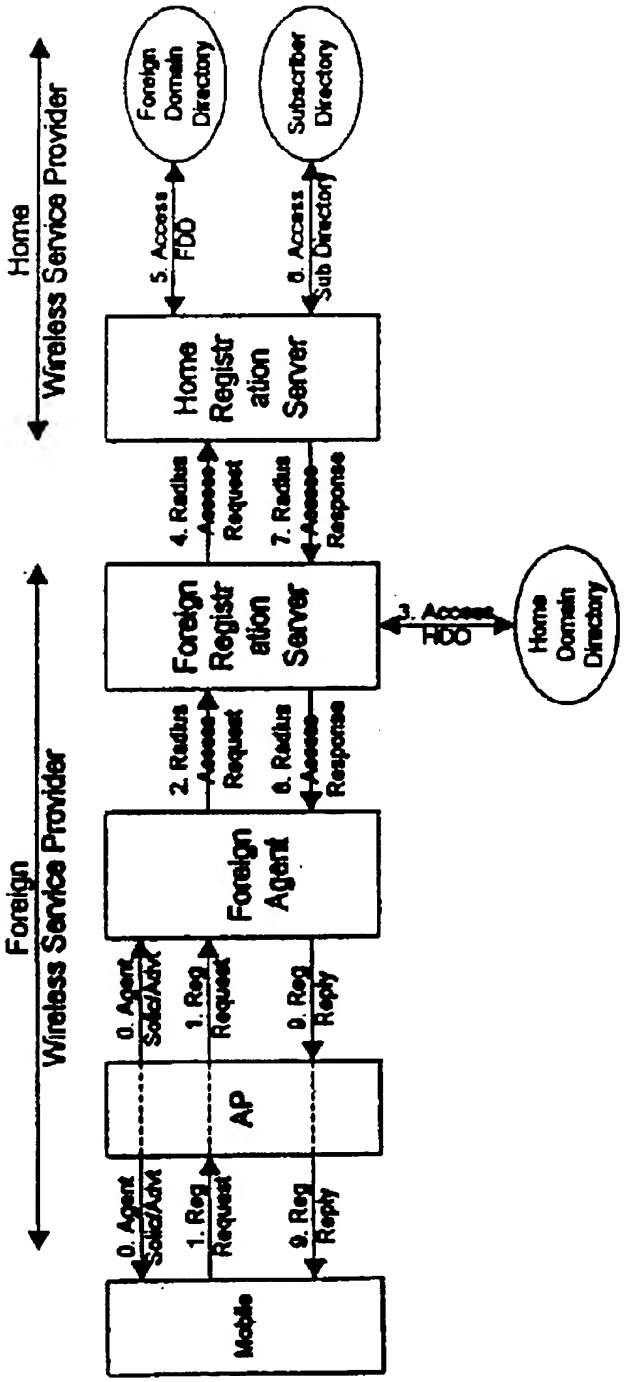

Home Wireless Service Provider
Foreign Wireless Service Provider
Foreign Domain Directory
Subscriber Directory
5. Access FDD
6. Access Sub Directory
Home Registration Server
4. Radius Access Request
7. Radius Access Response
Foreign Registration Server
3. Access FDD
Home Domain Directory
2. Radius Access Request
8. Radius Access Response
Foreign Agent
0. Agent Solic/Adv
1. Reg Request
9. Reg Reply
AP
0. Agent Solic/Adv
1. Reg Request
9. Reg Reply
Mobile

FIG. 17

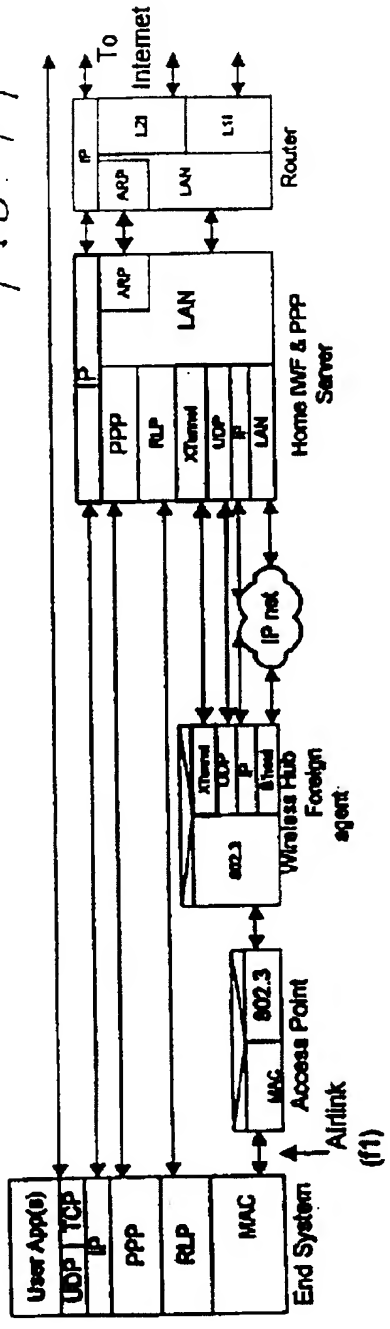

To Internet
L3
L1
IP
ARP
LAN
Router
ARP
LAN
IP
PPP
RLP
XTunnel
UDP
IP
LAN
Home IWF & PPP Server
IP net
XTunnel
UDP
IP
Ethnet
802.3
Wireless Hub
Foreign agent
802.3
MAC
Access Point
Airlink
(f1)
User App(s)
TCP
UDP
IP
PPP
RLP
MAC
End System

FIG. 18

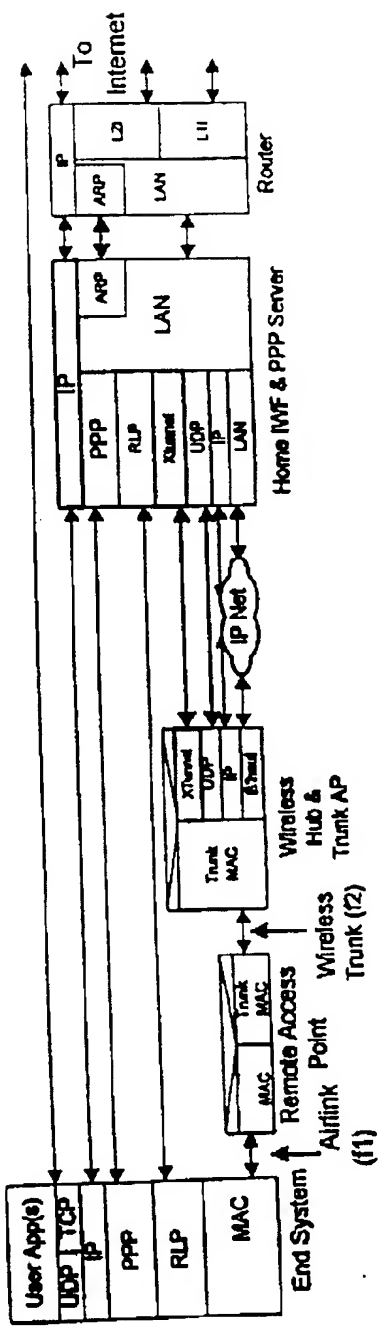

To Internet
L3
L1
IP
ARP
LAN
Router
ARP
LAN
IP
PPP
RLP
XTunnel
UDP
IP
LAN
Home IWF & PPP Server
IP Net
XTunnel
UDP
IP
Ethnet
Trunk MAC
Wireless Hub & Trunk AP
Wireless Trunk (f2)
Trunk MAC
MAC
Remote Access Point
Airlink
(f1)
User App(s)
TCP
UDP
IP
PPP
RLP
MAC
End System

FIG. 19

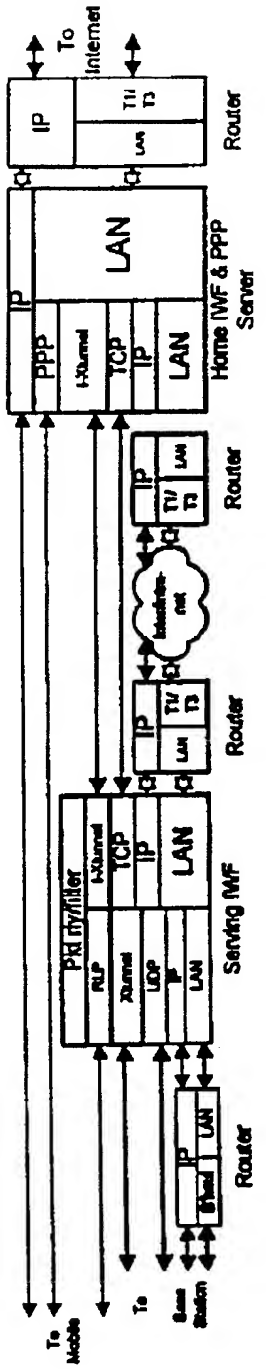

To Internet
IP
TV
LAN
Router
LAN
IP
PPP
L2tunnel
TCP
IP
LAN
Home IWF & PPP Server
Router
Internet
Router
Pkt mx/filter
RLP
L2tunnel
TCP
IP
UDP
IP
LAN
Serving IWF
Router
Ethernet
To Mobile
To
Base Station

FIG. 20

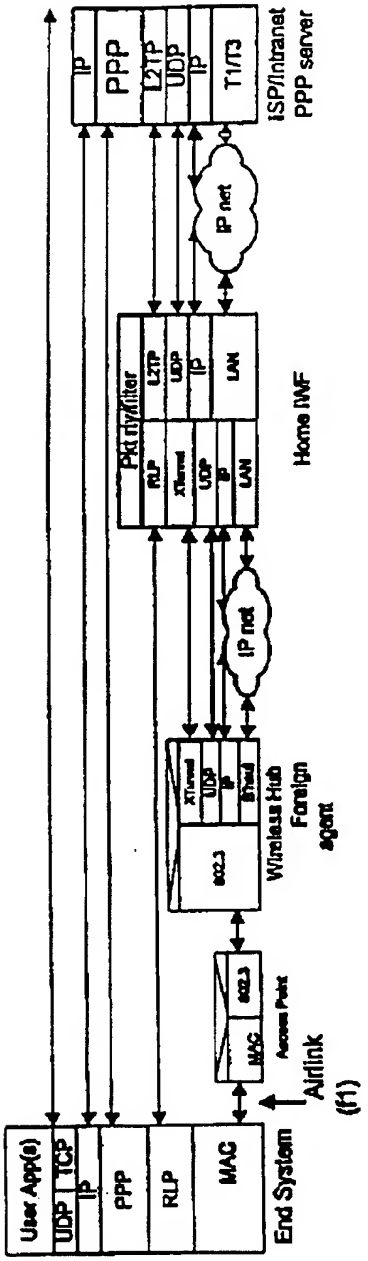

IP
PPP
L2TP
UDP
IP
T1/T3
ISP/Intranet PPP server
IP net
Pkt fly/filter
RLP
Ethernet
UDP
IP
LAN
Home IWF
IP net
Ethernet
UDP
IP
802.3
Wireless Hub Foreign agent
802.3
MAC
Access Point
Airlink (f1)
User App(s)
UDP
TCP
IP
PPP
RLP
MAC
End System

FIG 21

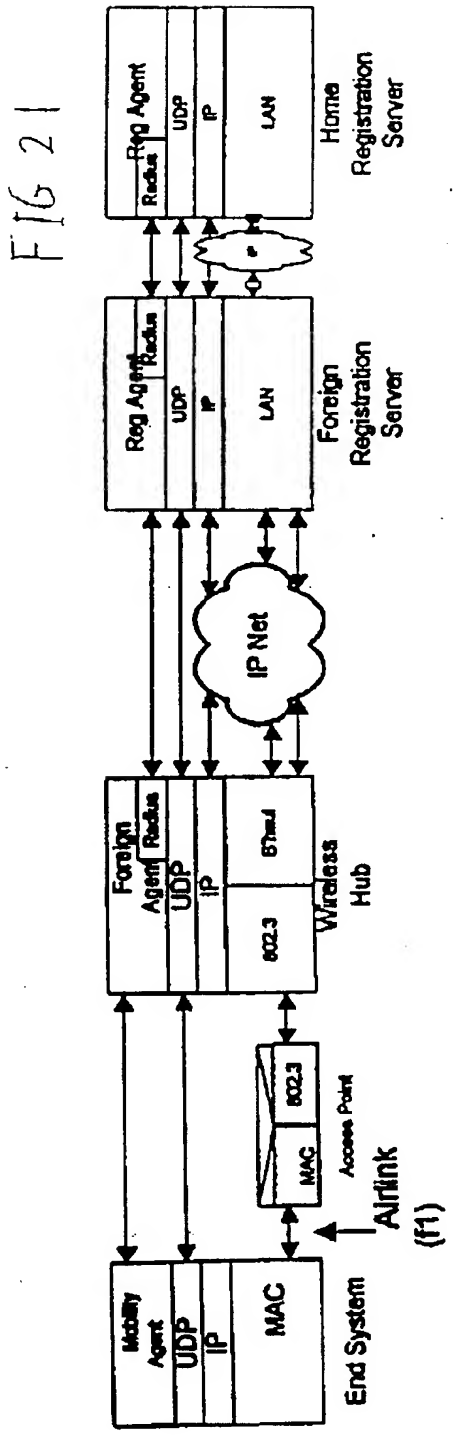

Reg Agent
Radius
UDP
IP
LAN
Home Registration Server
Reg Agent
Radius
UDP
IP
LAN
Foreign Registration Server
IP Net
Foreign Agent
Radius
UDP
IP
Ethernet
802.3
Wireless Hub
802.3
MAC
Access Point
Airlink (f1)
Mobility Agent
UDP
IP
MAC
End System

FIG. 22

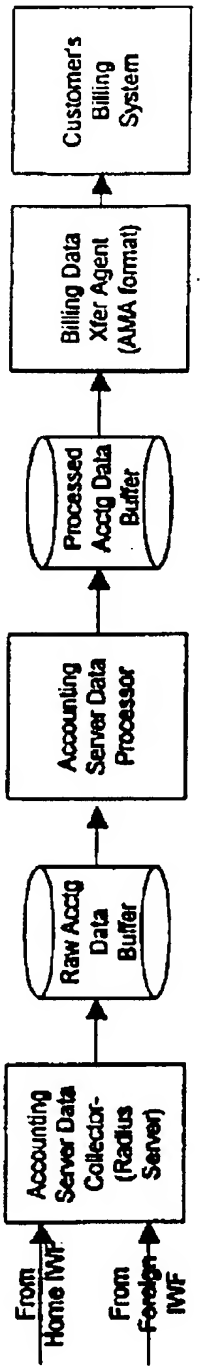

From Home IWF
From Foreign IWF
Accounting Server Data Collector- (Radius Server)
Raw Acctg Data Buffer
Accounting Server Data Processor
Processed Acctg Data Buffer
Billing Data Xfer Agent (AMA format)
Customer's Billing System

FIG. 23

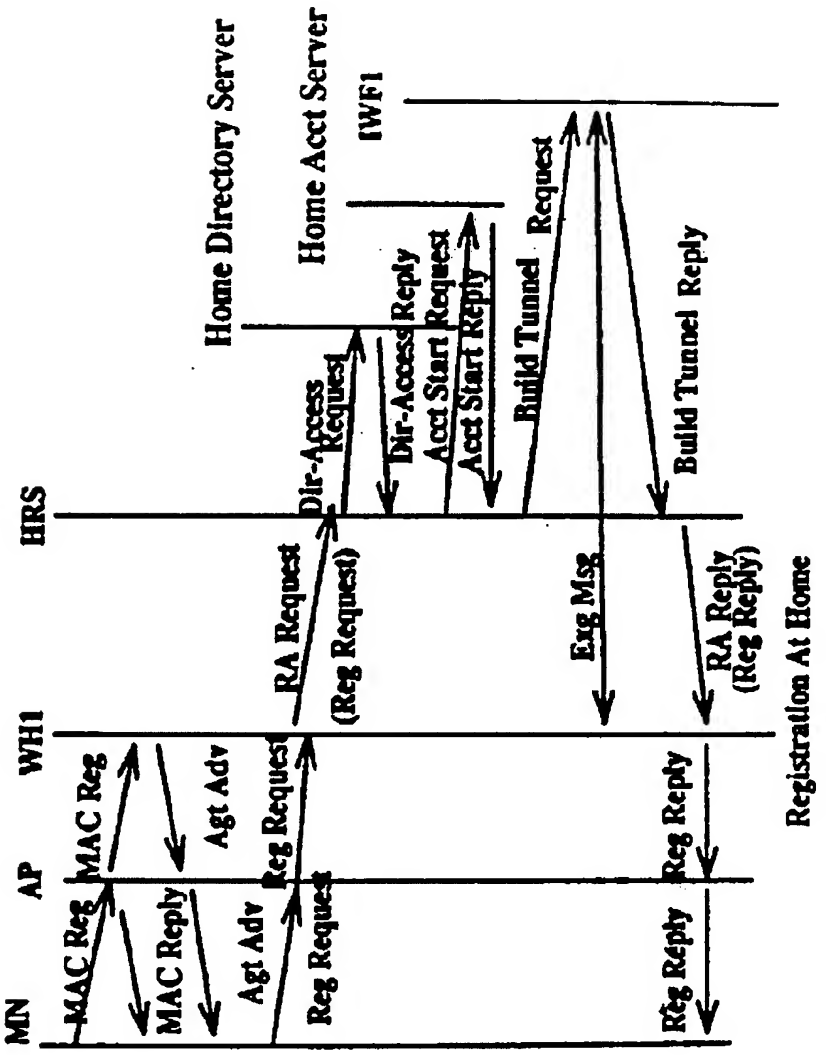

Home Directory Server
Home Acct Server
IWF1
HRS
WH1
AP
MN
Dir-Access Request
Dir-Access Reply
Acct Start Request
Acct Start Reply
Build Tunnel Request
Build Tunnel Reply
RA Request (Reg Request)
Exg Msg
RA Reply (Reg Reply)
MAC Reg
Agt Adv
Reg Request
Reg Reply
MAC Reg
MAC Reply
Agt Adv
Reg Request
Rfg Reply
Registration At Home

FIG. 24

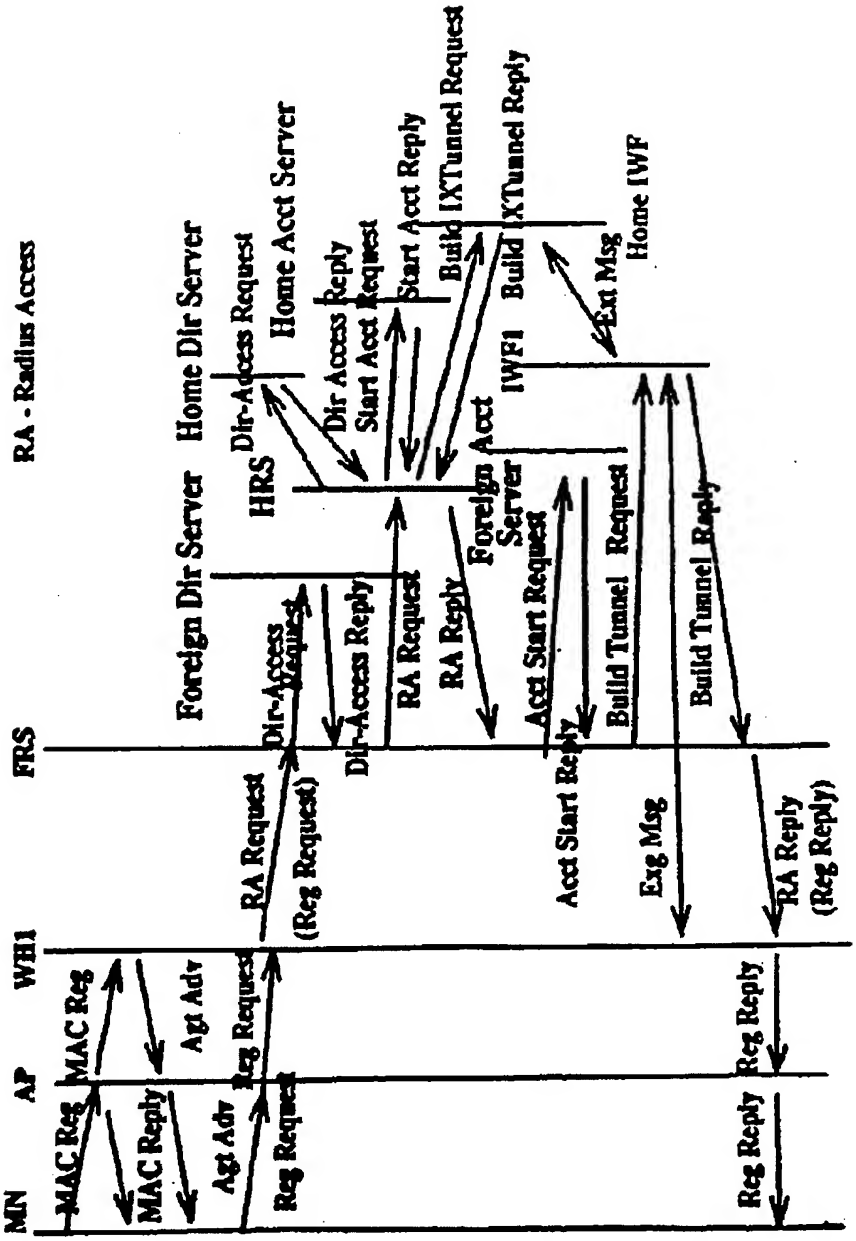

MN
AP
WB1
FRS
RA - Radius Access
Foreign Dir Server
Home Dir Server
HRS
Home Acct Server
Home IWF
MAC Req
MAC Reply
Agt Adv
Reg Request
Reg Reply
RA Request
(Reg Request)
RA Reply
(Reg Reply)
Dir-Access Request
Dir-Access Reply
Dir Access Request
Dir Access Reply
RA Request
RA Reply
Start Acct Request
Start Acct Reply
Build IXTunnel Request
Build IXTunnel Reply
Foreign Acct Server
IWF1
Ext Msg
Acct Start Request
Acct Start Reply
Build Tunnel Request
Build Tunnel Reply
Esg Msg

FIG. 25

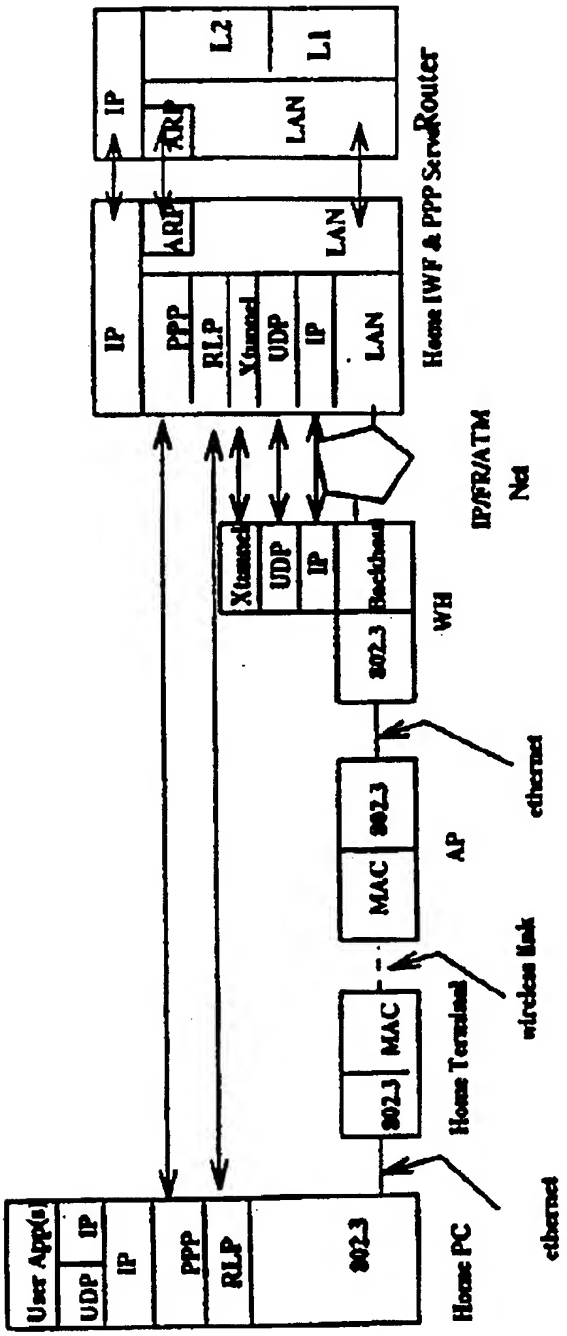

L2
L1
IP
ARP
LAN
Router
ARP
LAN
IP
PPP
RLP
Xtunnel
UDP
IP
LAN
Home IWF & PPP Server
IP/FR/ATM
Net
Xtunnel
UDP
IP
Backhaul
802.3
WH
802.3
MAC
AP
ethernet
wireless link
802.3
MAC
Home Terminal
ethernet
User App(s)
UDP
IP
IP
PPP
RLP
802.3
Home PC

FIG. 26

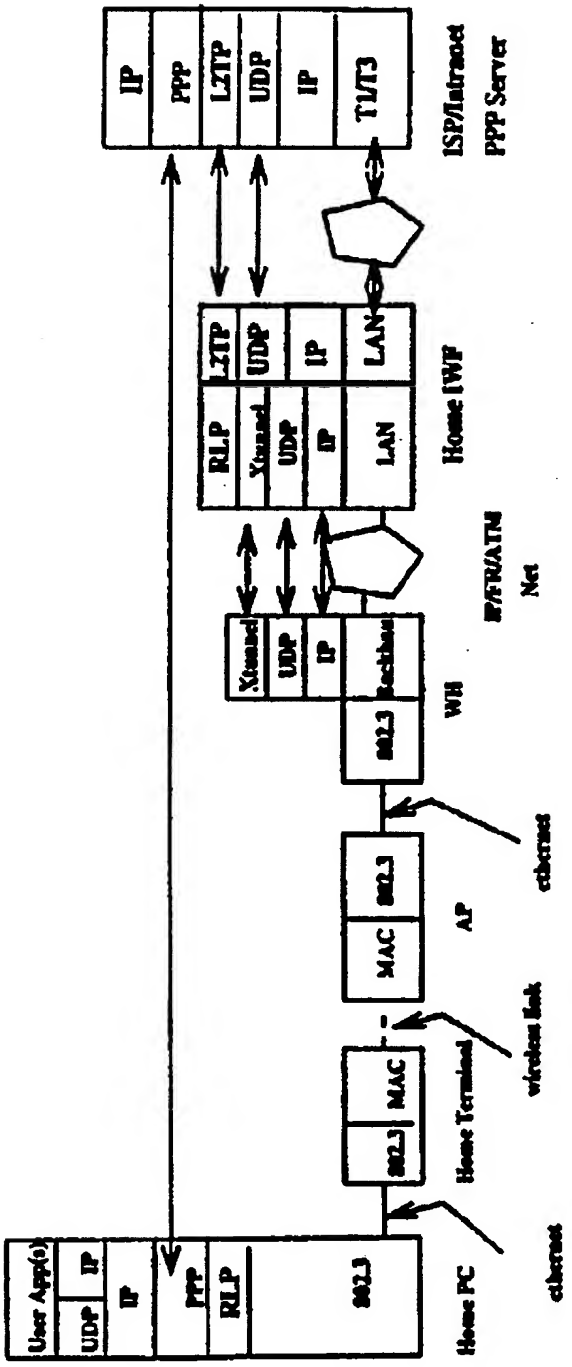

IP
PPP
L2TP
UDP
IP
T1/T3
ISP/Intranet
PPP Server
L2TP
UDP
IP
LAN
RLP
Xmux
UDP
IP
LAN
Home IWF
Xmux
UDP
IP
Backbone
802.3
WII
IP/FR/ATM
Net
802.3
MAC
AP
ethernet
802.3
MAC
Home Terminal
wireless link
802.3
Home PC
ethernet
User App(s)
UDP
IP
IP
PPP
RLP
802.3

FIG. 27

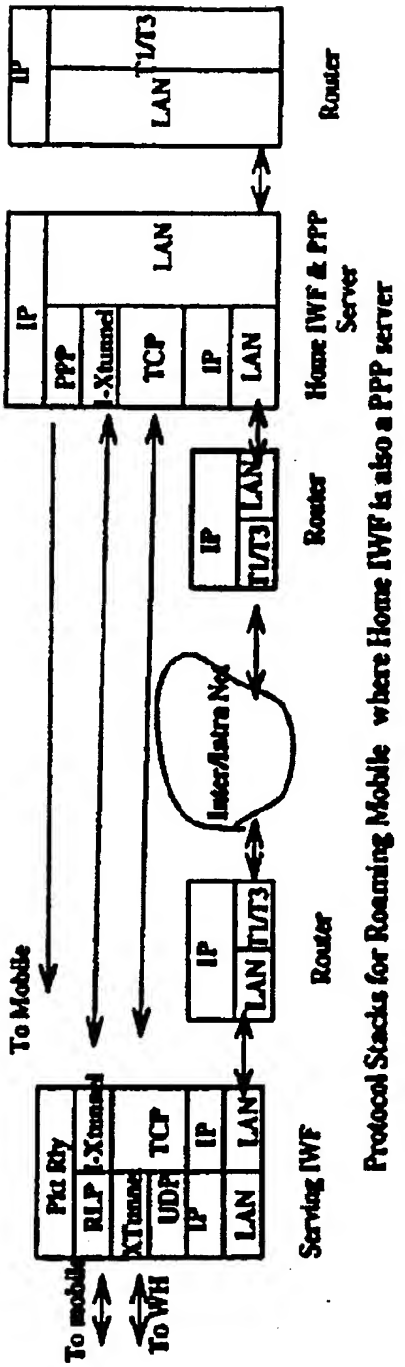
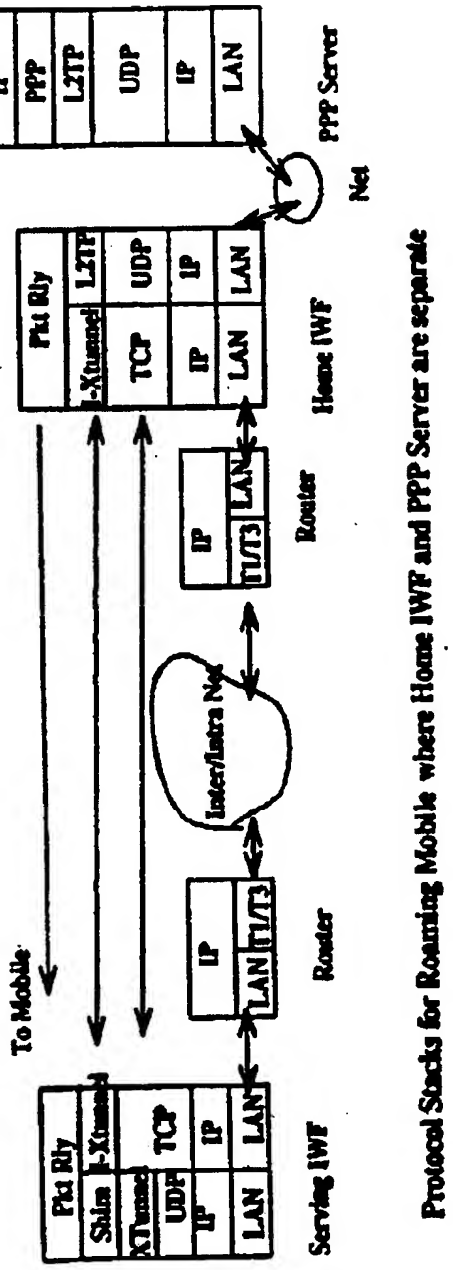

IP
LAN
T1/T3
Router
IP
PPP
I-Xtunnel
TCP
IP
LAN
LAN
Home IWF & PPP Server
IP
LAN
T1/T3
Router
Inter/Intra Net
IP
LAN
T1/T3
Router
To Mobile
Pkt Rty
RLP
I-Xtunnel
TCP
IP
LAN
XTunnel
UDP
IP
LAN
Serving IWF
To mobile
To WH
Protocol Stacks for Roaming Mobile where Home IWF is also a PPP server

FIG. 28


IP
PPP
L2TP
UDP
IP
LAN
PPP Server
Net
Pkt Rly
L-Xtunnel
L2TP
UDP
IP
LAN
TCP
IP
LAN
Home IWF
IP
11/13
LAN
Router
Internet/Intra Net
To Mobile
IP
LAN
11/13
Router
Pkt Rly
L-Xtunnel
Shim
XTunnel
TCP
UDP
IP
IP
LAN
LAN
Serving IWF
Protocol Stacks for Roaming Mobile where Home IWF and PPP Server are separate

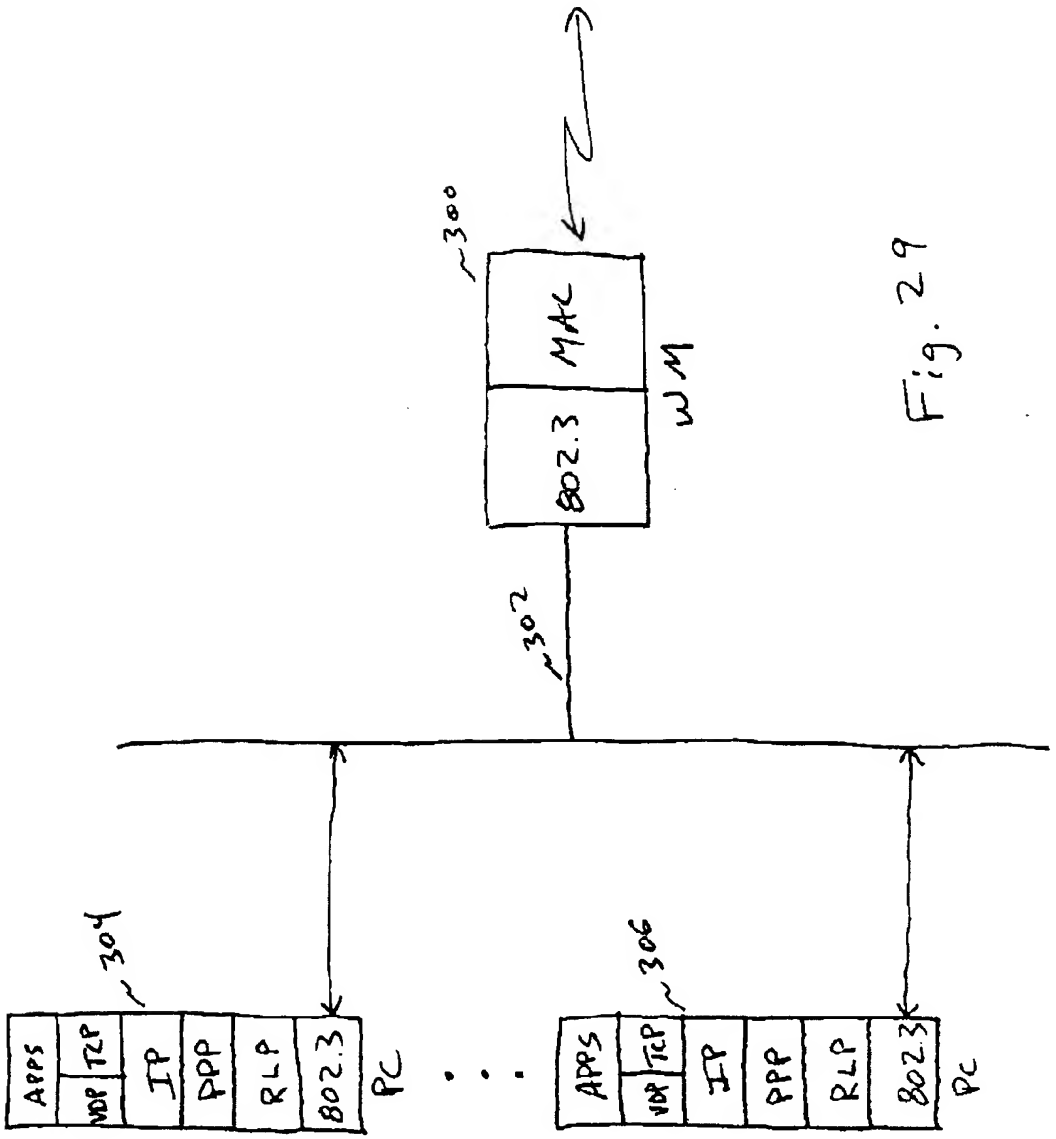

300
MAC
802.3
WM
302
304
APPS
TCP
UDP
IP
PPP
RLP
802.3
PC
306
APPS
TCP
UDP
IP
PPP
RLP
802.3
PC

Fig. 29

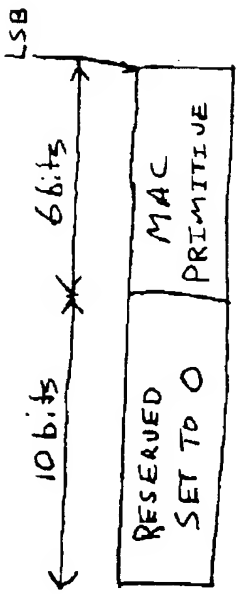

LSB
6 bits
10 bits
MAC PRIMITIVE
RESERVED SET TO 0

Fig. 31

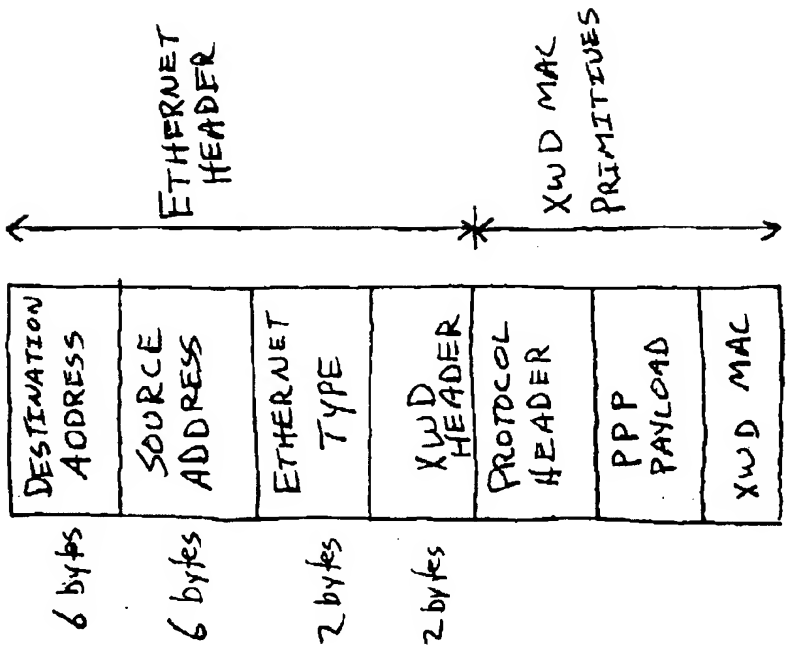

ETHERNET HEADER
XWD MAC PRIMITIVES
DESTINATION ADDRESS
SOURCE ADDRESS
ETHERNET TYPE
XWD HEADER
PROTOCOL HEADER
PPP PAYLOAD
XWD MAC
6 bytes
6 bytes
2 bytes
2 bytes

Fig. 30

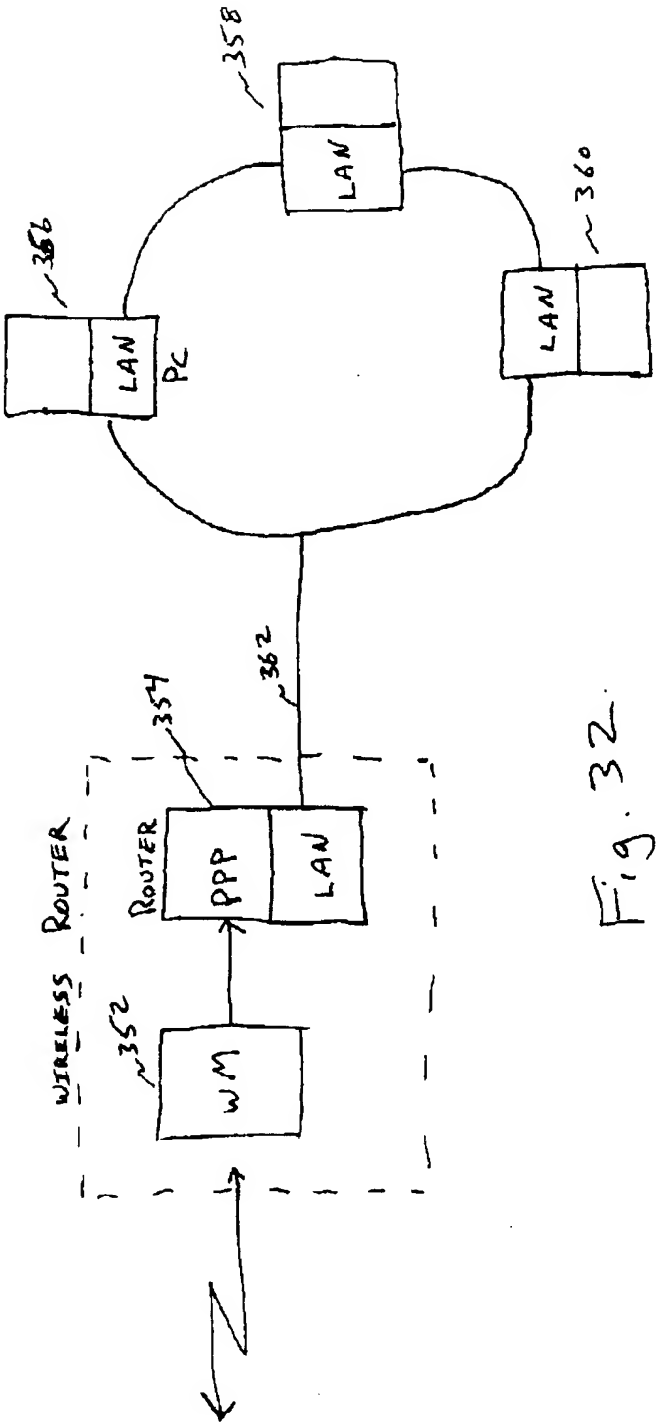
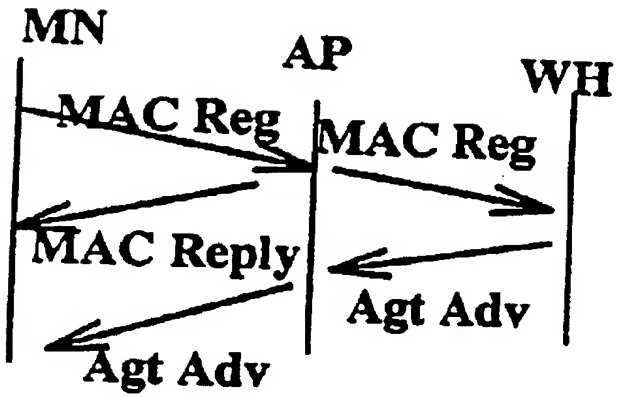

358
LAN
360
LAN
356
LAN
PC
362
354
ROUTER
PPP
LAN
WIRELESS ROUTER
352
WM

Fig. 32

FIG. 33



Local Handoff

FIG 34

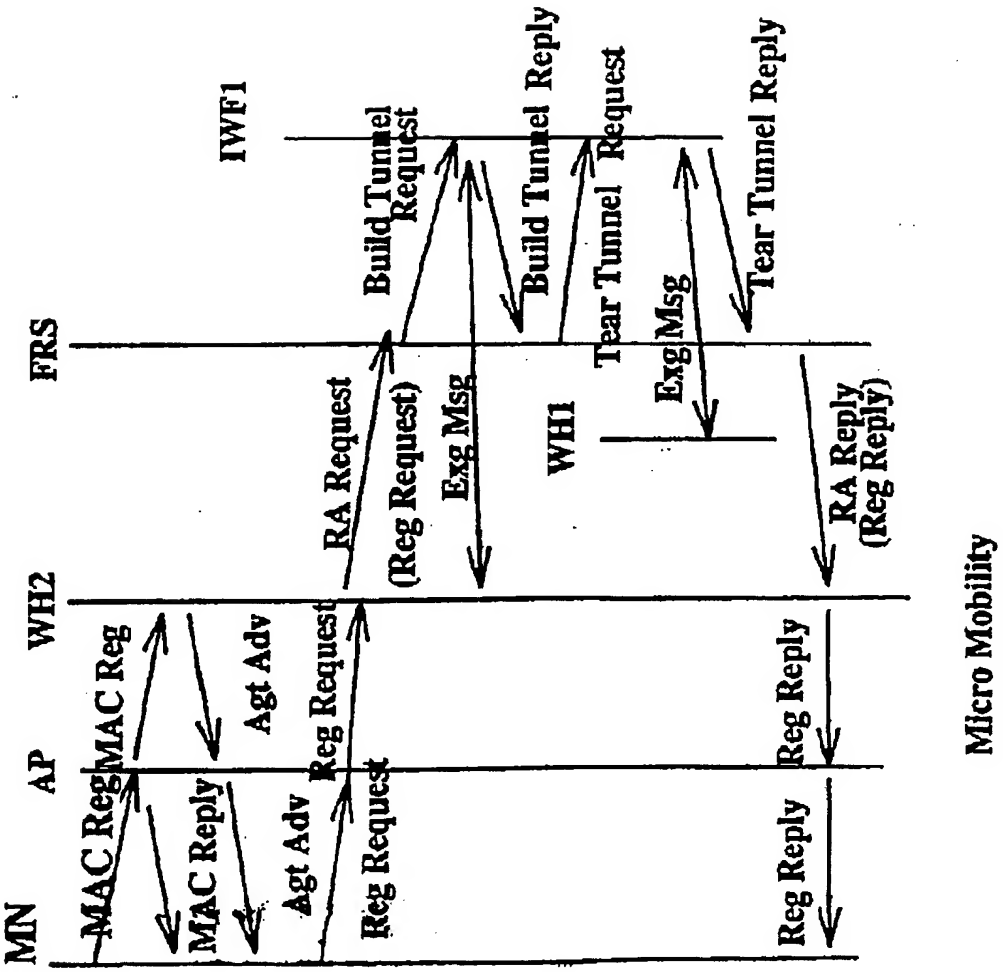

MN
AP
WH2
FRS
IWF1
WH1
MAC Reg
MAC Reply
Agt Adv
Reg Request
RA Request
(Reg Request)
Exg Msg
Build Tunnel Request
Build Tunnel Reply
Tear Tunnel Request
Exg Msg
Tear Tunnel Reply
RA Reply
(Reg Reply)
Reg Reply
Reg Reply
Micro Mobility

FIG. 35

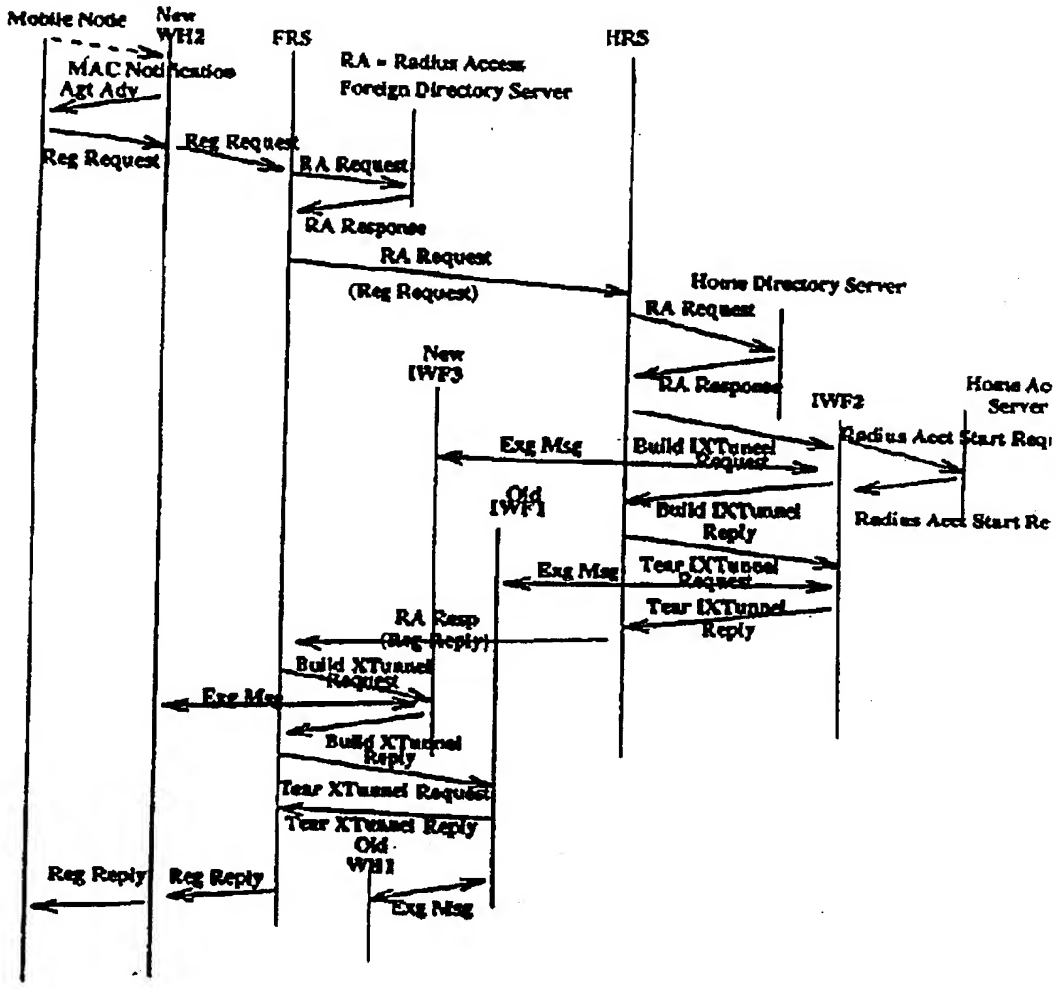

Mobile Node
New WH2
FRS
RA = Radius Access
Foreign Directory Server
HRS
MAC Notification
Agt Adv
Reg Request
Reg Request
RA Request
RA Response
RA Request
(Reg Request)
Home Directory Server
RA Request
RA Response
New IWF3
IWF2
Home Ac Server
Exg Msg
Build IXTunnel Request
Radius Acct Start Req
Old IWF1
Build IXTunnel Reply
Radius Acct Start Re
Exg Msg
Tear IXTunnel Request
Tear IXTunnel Reply
RA Resp
(Reg Reply)
Build XTunnel Request
Exg Msg
Build XTunnel Reply
Tear XTunnel Request
Tear XTunnel Reply
Old WH1
Reg Reply
Reg Reply
Exg Msg

FIG. 36

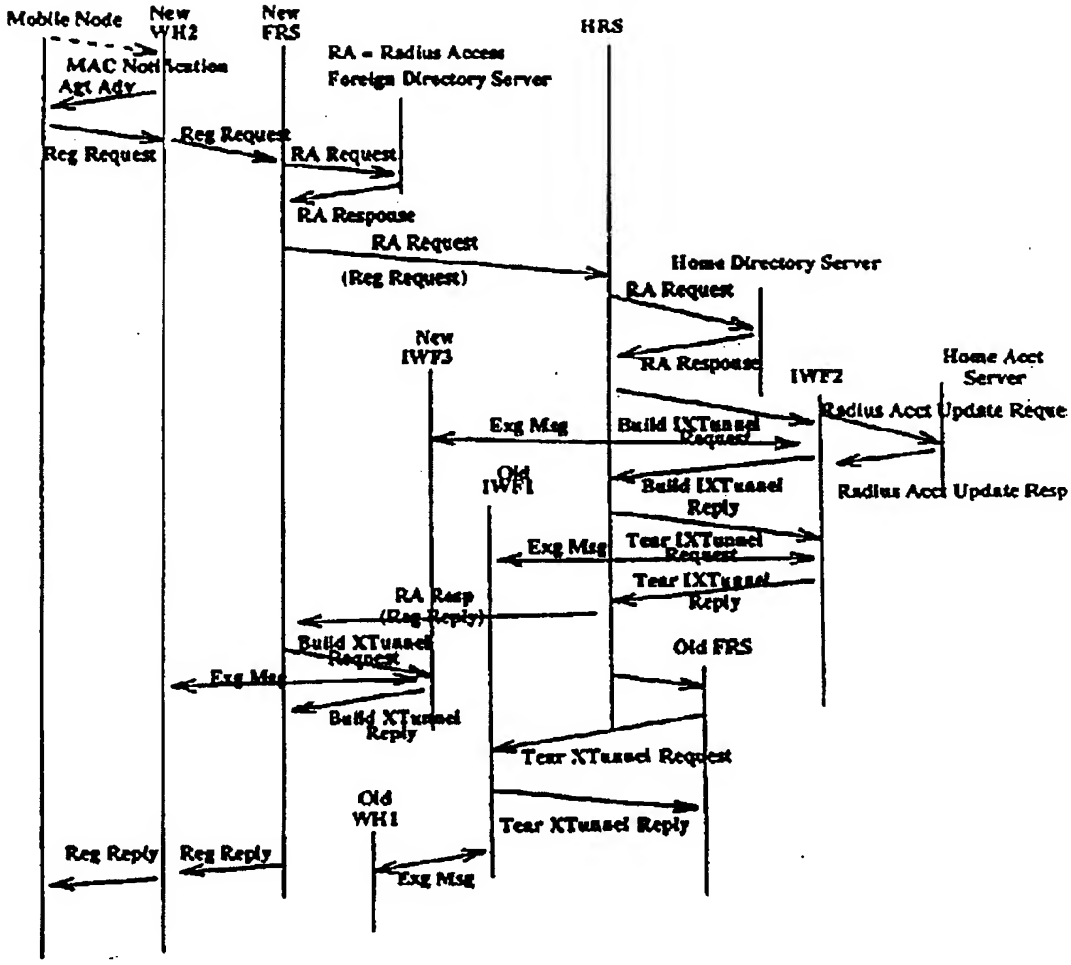
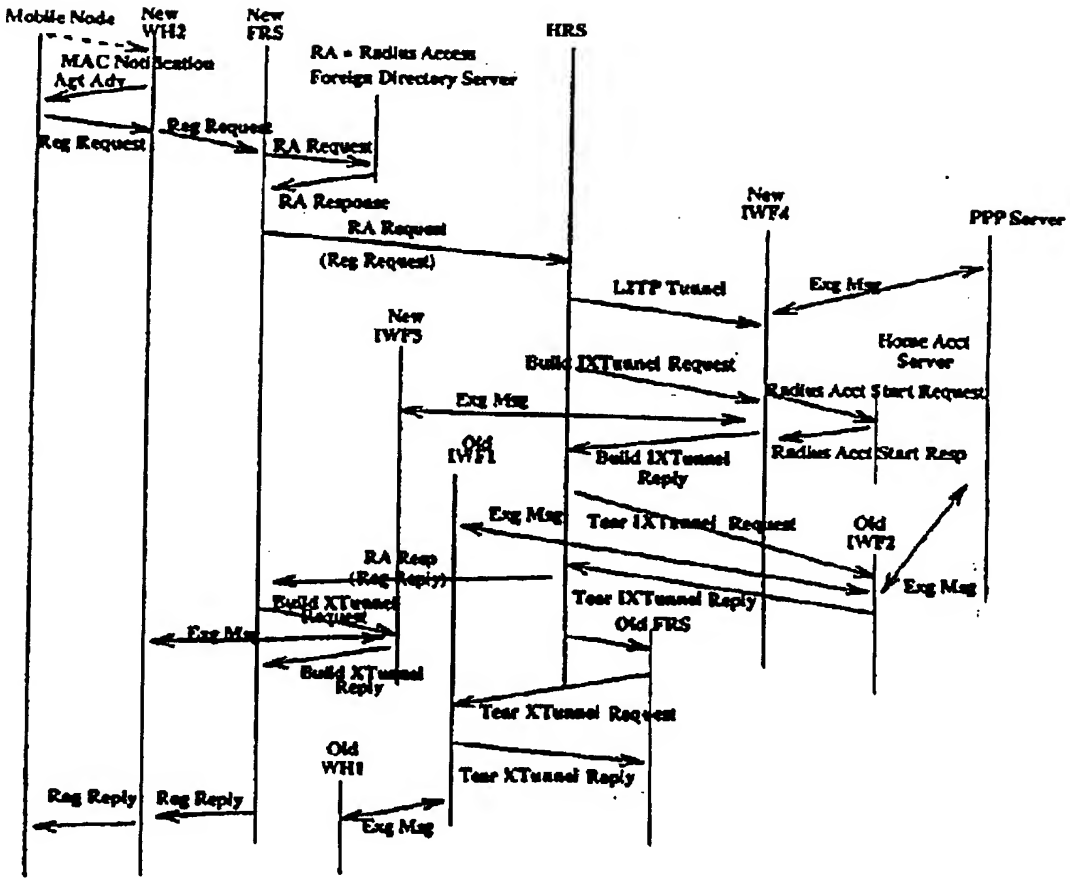

Mobile Node
New WH2
New FRS
HRS
RA = Radius Access
Foreign Directory Server
MAC Notification
Agt Adv
Reg Request
Reg Request
RA Request
RA Response
RA Request
(Reg Request)
Home Directory Server
RA Request
RA Response
New IWF3
IWF2
Home Acct Server
Radius Acct Update Reque
Exg Msg
Build IXTunnel Request
Old IWF1
Build IXTunnel Reply
Radius Acct Update Resp
Exg Msg
Tear IXTunnel Request
Tear IXTunnel Reply
RA Resp
(Reg Reply)
Build XTunnel Request
Old FRS
Exg Msg
Build XTunnel Reply
Tear XTunnel Request
Old WH1
Tear XTunnel Reply
Reg Reply
Reg Reply
Exg Msg

FIG. 37


Mobile Node
New WH2
New FRS
HRS
RA = Radius Access
Foreign Directory Server
MAC Notification
Agt Adv
Reg Request
Reg Request
RA Request
RA Response
RA Request
(Reg Request)
New IWF4
PPP Server
L2TP Tunnel
Exg Msg
New IWF3
Home Acct Server
Build IXTunnel Request
Radius Acct Start Request
Exg Msg
Old IWF1
Radius Acct Start Resp
Build IXTunnel Reply
Exg Msg
Tear IXTunnel Request
Old IWF2
RA Resp
(Reg Reply)
Exg Msg
Tear IXTunnel Reply
Build XTunnel Request
Old FRS
Exg Msg
Build XTunnel Reply
Tear XTunnel Request
Old WH1
Tear XTunnel Reply
Reg Reply
Reg Reply
Exg Msg

1. Abstract

A wireless data network which provides communications with a Pier to Pier Protocol server is disclosed. The network includes a home network that includes a home mobile switching center, a wireless modem and one or more end system. The wireless modem and the end systems are connected together via an ethernet link. The network also includes a PPP server, wherein PPP information sent from PPP server for the end systems is encapsulated by the wireless modem in an ethernet frame and sent to the end systems via the ethernet link.

2. Representative Drawing

FIG. 2